VMware SD-WAN by VeloCloud-Administratorhandbuch

VMware SD-WAN by VeloCloud 3.4

vmware®

Die aktuellste technische Dokumentation finden Sie auf der VMware-Website unter:

https://docs.vmware.com/de/

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware Global, Inc.
Zweigniederlassung Deutschland
Willy-Brandt-Platz 2
81829 München
Germany
Tel.: +49 (0) 89 3706 17 000
Fax: +49 (0) 89 3706 17 333
www.vmware.com/de

Inhalt

Informationen zum Administratorhandbuch für VMware SD-WAN by VeloCloud

1

Das Administratorhandbuch für VMware SD-WAN™ by VeloCloud® enthält Informationen zu VMware SD-WAN Orchestrator und den wichtigsten VMware SD-WAN-Konfigurationseinstellungen, einschließlich Netzwerk, Netzwerkdienste, Edges, Profile und Kunden, die SD-WAN Orchestrator verwenden.

Zielgruppe

Dieses Handbuch richtet sich an Netzwerkadministratoren, Netzwerkanalysten und IT-Administratoren, die für die Bereitstellung, Überwachung und Verwaltung des Netzwerks der Unternehmenszweigstelle verantwortlich sind.

Neuheiten

2

Neuheiten in Version 3.4.1

Funktion	Beschreibung
Unterstützung für private Segmente	Wird für Datenverkehrsströme mit beschränkter Sichtbarkeit verwendet, um den Datenschutzanforderungen der Endbenutzer Rechnung zu tragen. Weitere Informationen finden Sie unter Kapitel 7 Konfigurieren von Segmenten.
Verbesserung der Syslog-Firewallprotokollierung	Wenn die Option **Alle Segmente (All Segments)** aktiviert ist, kann der Syslog-Collector Firewallprotokolle aus allen Segmenten empfangen. Darüber hinaus wird die Firewallprotokollmeldung um neue Nachrichtenfelder erweitert. Weitere Informationen finden Sie unter Konfigurieren von Syslog-Einstellungen auf der Profilebene.
Verbesserung von MPLS CoS	Beim Konfigurieren von MPLS CoS können Sie strengen IP-Vorrang erzwingen, um die Dienstklassen in weniger Klassen im Netzwerk Ihres Dienstanbieters zusammenzufassen. Weitere Informationen finden Sie unter Konfigurieren von MPLS-CoS.

Neuheiten in Version 3.4

Funktion	Beschreibung
Bedingter Backhaul	Wenn der bedingte Backhaul aktiviert ist, kann der Edge ein Failover von internetgebundenem Datenverkehr (direkter Internetdatenverkehr und Datenverkehr für Cloud-Sicherheit über IPsec) auf MPLS-Links durchführen, wenn keine öffentlichen Internet-Links verfügbar sind. Weitere Informationen finden Sie unter Konfigurieren von Edge-Clustering und Konfigurieren des Aktionsnetzwerkdiensts.
Konfigurieren von DSL-Einstellungen	Unterstützung ist verfügbar für das Metanoia xDSL SFP-Modul (MT 5311), ein hochintegriertes SFP-Bridged-Modem, das eine steckbare SFP-kompatible Schnittstelle bietet, um vorhandene DSL IAD- oder Home-Gateway-Geräte auf Dienste mit höherer Bandbreite aufzurüsten. Weitere Informationen finden Sie unter Konfigurieren von DSL-Einstellungen.
Updates für Edge-Clustering	Aktualisierte Informationen zu Edge-Clustering und der Funktionsweise finden Sie in den folgenden Abschnitten: Info zu Edge-Clustering, Funktionsweise von Edge-Clustering.
Benutzerdefinierte Informationen für Edge	Ermöglicht Standard-Admin und Superuser der Enterprise/MSP/Operatorrollen (Benutzer mit UPDATE_EDGE-Berechtigung), benutzerdefinierte Informationen für einen Edge hinzuzufügen oder zu aktualisieren. Weitere Informationen finden Sie unter Bereitstellen eines neuen Edge.

Funktion	Beschreibung
Edge-WLAN-Verbesserungen	Auf der Edge-Ebene können auf der Grundlage des Edge-Modells und des für den Edge konfigurierten Lands ein Funkband und ein Kanal ausgewählt werden, die für den Edge unterstützt werden. Weitere Informationen finden Sie unter Konfigurieren von Außerkraftsetzungen für WLAN-Funk.
Verbesserte MPLS CoS	Beim Konfigurieren von MPLS CoS gibt es eine Verbesserung bei der Zuordnung der DSCP-Tags. Sie sollten DSCP-Tags mit gleicher IP-Priorität zur gleichen Dienstklasse zuordnen. Weitere Informationen finden Sie unter Konfigurieren von MPLS-CoS.
Unternehmensberichte	Ermöglicht das Erstellen von Berichten mit der Gesamtübersicht des Netzwerks sowie Informationen zu SD-WAN-Datenverkehr und -Transportverteilung. Die Berichte ermöglichen die Analyse Ihres Netzwerks. Weitere Informationen finden Sie unter Überwachen von Berichten.
Fehlerbehebung bei Hub-Clustering	Es gibt zwei Fehlerbehebungsfunktionen für Hub-Clustering (Verfolgung der Anzahl der Spoke-Neuzuweisungen und Neuverteilung von Spokes auf Hubs im Cluster). Diese Funktionen können für die Fehlerbehebung oder Wartung verwendet werden, um alle Spokes in einem Hub-Cluster neu zu verteilen. Weitere Informationen hierzu finden Sie unter Fehlerbehebung bei Edge-Clustering.
Verbesserungen bei NAT auf dem Edge	Benutzer können Quell-NAT basierend auf dem Ziel oder Ziel-NAT basierend auf der Quelle angeben, oder Benutzer können die Quell- und Ziel-IP für NAT in einem Paket angeben. Weitere Informationen finden Sie unter LAN-seitige NAT-Regeln auf Edge-Ebene.
NetFlow-Datenerweiterungen	Ermöglicht dem Benutzer, das Exportintervall für die Tunnelstatusvorlage zu konfigurieren. Weitere Informationen finden Sie unter Konfigurieren von Netflow-Einstellungen auf der Profilebene.
Neue Remotediagnosetests für 510 LTE und 610	Der Diagnosetest „LTE-Modeminformationen“ (LTE Modem Information) ist für konfigurierte Edge 510-LTE-Geräte verfügbar. Dieser Test ruft Diagnosedaten ab, wie z. B. Signalstärke, Verbindungsinformationen usw. Weitere Informationen finden Sie unter Konfigurieren von Geräteeinstellungen.
Objektgruppen	Eine Objektgruppe besteht aus einem Bereich von IP-Adressen oder Portnummern. Wenn Sie Unternehmensrichtlinien und Firewallregeln erstellen, können Sie die Regeln für einen Bereich von IP-Adressen oder einen Bereich von TCP/UDP-Ports definieren, indem Sie die Objektgruppen in die Regeldefinitionen einschließen. Weitere Informationen finden Sie unter Kapitel 17 Objektgruppen.
Statusbehaftete Firewall	Eine statusbehaftete Firewall überwacht und verfolgt den Betriebszustand und die Merkmale aller Netzwerkverbindungen, die über die Firewall kommen, und verwendet diese Informationen, um zu ermitteln, welche Netzwerkpakete die Firewall passieren sollen. Weitere Informationen finden Sie unter Konfigurieren einer Firewallregel.
Unterstützung für X710/XL710-Netzwerkkarte mit DPDK und SR-IOV	SR-IOV- und DPDK-Unterstützung für die neue Intel X710/XL710-Netzwerkkarte. Siehe ■ Bereitstellungsvoraussetzungen für den virtuellen VMware SD-WAN Edge ■ Installieren des virtuellen VMware SD-WAN-Edge
Syslog-Firewallprotokollierung	Ermöglicht die Erfassung von SD-WAN Orchestrator-gebundenen Ereignissen und Firewallprotokollen, die von einem Unternehmens-SD-WAN Edges stammen, in einer oder mehreren zentralen Remote-Syslog-Collector-Instanzen (Servern) im nativen Syslog-Format. Weitere Informationen finden Sie unter Konfigurieren von Syslog-Einstellungen auf der Profilebene und Konfigurieren von Syslog-Einstellungen auf der Edge-Ebene.

Funktion	Beschreibung
Tokenbasierte Authentifizierung	Die Benutzer können mithilfe von Token anstelle der sitzungsbasierten Authentifizierung auf die SD-WAN Orchestrator-APIs zugreifen. Als Operator-Superuser können Sie die API-Token für Unternehmensbenutzer verwalten. Weitere Informationen hierzu finden Sie unter API-Token.
Webhook-Warnungen	Webhooks liefern Daten an andere Anwendungen, die von bestimmten Ereignissen mithilfe von HTTP POST ausgelöst werden. Wenn ein Ereignis eintritt, sendet die Quelle eine HTTP-Anfrage an die zielseitige Anwendung, die für den Webhook konfiguriert ist. Weitere Informationen finden Sie unter Webhooks.

Vorherige VMware SD-WAN by VeloCloud-Versionen

Um die Produktdokumentation für frühere VMware SD-WAN by VeloCloud-Versionen zu erhalten, wenden Sie sich an Ihren VMware SD-WAN by VeloCloud-Ansprechpartner.

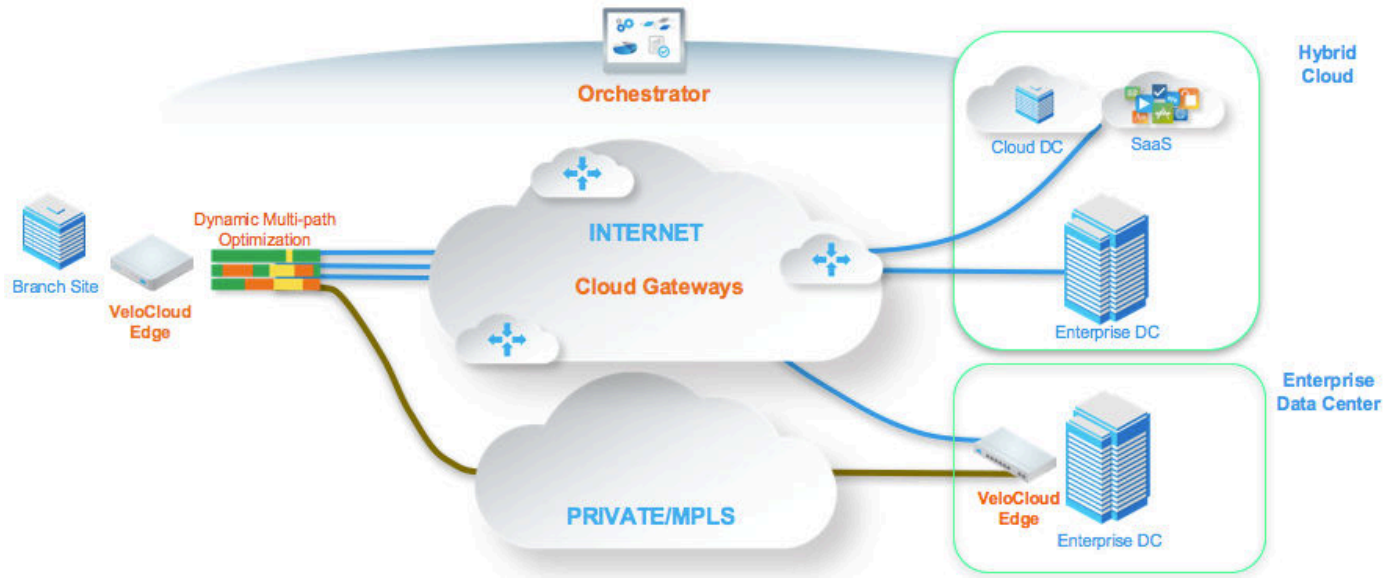
Übersicht

3

VMware SD-WAN by VeloCloud ist eine Cloud-basierte Netzwerkdienstlösung, die es Sites ermöglicht, schnell unternehmensweiten Zugriff auf Legacy- und Cloud-Anwendungen sowohl über private Netzwerke als auch über Internet-Breitband bereitzustellen.

In der Cloud bereitgestelltes softwaredefiniertes WAN sichert Unternehmen die Leistung von Cloud-Anwendungen über das Internet und Hybrid-WAN und vereinfacht gleichzeitig Bereitstellungen und reduziert Kosten.

Die folgende Abbildung zeigt die Komponenten der VMware SD-WAN-Lösung orangefarben an. Die Komponenten werden in den folgenden Abschnitten näher beschrieben.



Um sich mit der Basiskonfiguration und der Edge-Aktivierung vertraut zu machen, erhalten Sie weitere Informationen unter Kapitel 20 Schnellstartkonfiguration.

Dieses Kapitel enthält die folgenden Themen:

- Lösungskomponenten
- Funktionen
- Tunnel-Overhead und MTU
- Netzwerktopologien

Lösungskomponenten

In diesem Abschnitt werden VMware SD-WAN-Lösungskomponenten beschrieben.

VMware SD-WAN Edge

Ein „Thin Edge“, der ohne „IT-Berührung“ über die Cloud bereitgestellt wurde, um für Ihre Apps und virtualisierten Dienste sichere und optimierte Konnektivität zu liefern. Bei den SD-WAN Edges-Instanzen handelt es sich um Zero-Touch-Geräte der Enterprise-Klasse oder virtuelle Software, die sichere und optimierte Konnektivität für private, öffentliche und hybride Anwendungen, Computing-Dienste und virtualisierte Dienste bereitstellt. SD-WAN Edges-Instanzen führen neben dem Hosting von VNF-Diensten (Virtual Network Function) tiefgehende Anwendungserkennung, Anwendungs- und Paketsteuerung, Leistungsmetriken für bedarfsorientierte Standardisierung und End-to-End-QoS (Quality of Service) aus. Um Hochverfügbarkeit (HA) zu liefern, kann ein Edge-Paar bereitgestellt werden. Edges können in Branches, großen Sites und Datencentern bereitgestellt werden. Alle anderen Netzwerkinfrastrukturen werden bedarfsabhängig in der Cloud bereitgestellt.

VMware SD-WAN Orchestrator bietet zentralisierte unternehmensweite Konfigurations- und Echtzeitüberwachung und orchestriert den Datenfluss in und über das SDWAN-Overlay-Netzwerk. Darüber hinaus wird die Bereitstellung virtueller Dienste mit einem Mausklick über Edges, in zentralen und regionalen Enterprise-Service-Hubs und in der Cloud ermöglicht.

VMware SD-WAN Gateways

Das VMware SD-WAN-Netzwerk besteht aus Gateways, die an Netzwerk-Point-of-Presence-Punkten und in Cloud-Datencentern der obersten Ebene auf der ganzen Welt eingesetzt werden und SDWAN-Dienste bis „vor die Haustür“ von SaaS-, IaaS- und Cloud-Netzwerkdiensten sowie Zugang zu privaten Backbones bieten. Virtuelle Gateways mit mehreren Mandanten werden sowohl von VMware SD-WAN-Übergangs- als auch von Cloud-Dienstanbieter-Partnern bereitgestellt. Die Gateways bieten den Vorteil eines bedarfsgesteuerten, skalierbaren und redundanten Cloud-Netzwerks für optimierte Pfade zu Cloud-Zielen sowie für Anwendungen ohne Installation.

Ein Cloud-Edge kann auch mit SD-WAN Gateways konfiguriert werden, um einen Firewallschutz für eingehende Internetverbindungen zu bieten.

Funktionen

In diesem Abschnitt werden VMware SD-WAN-Funktionen beschrieben.

Dynamische Mehrfachpfadoptimierung

Die dynamische Mehrfachpfadoptimierung von VMware SD-WAN besteht aus automatischer Link-Überwachung, dynamischer Link-Steuerung und bedarfsorientierter Standardisierung.

Link-Steuerung und Standardisierung

Die dynamische, anwendungsorientierte Link-Steuerung pro Paket erfolgt automatisch auf der Grundlage der Geschäftspriorität der Anwendung, der eingebetteten Kenntnisse der Netzwerkanforderungen der Anwendung und der Echtzeitkapazität und -leistung der einzelnen Links. Die bedarfsorientierte Minderung einzelner Link-Degradierungen durch vorwärts gerichtete Fehlerkorrektur, Jitter-Pufferung und negativen Bestätigungs-Proxy schützt auch die Leistung prioritärer und netzwerksensitiver Anwendungen. Sowohl die dynamische Link-Steuerung pro Paket als auch die bedarfsorientierte Minderung bieten zusammen einen verlässlichen blockierenden und eingeschränkten Schutz in Sekundenbruchteilen, um die Anwendungsverfügbarkeit, die Leistung und das Endbenutzererlebnis zu verbessern.

Cloud-VPN

Das Cloud-VPN ist ein VPNC-konformes IPSec-VPN von Site zu Site, das mit einem Klick erreichbar ist. Dieses VPN verbindet VMware SD-WAN mit Non VMware SD-WAN Sites und stellt den Echtzeitstatus und die Integrität der Sites bereit. Das Cloud-VPN stellt eine dynamische Kommunikation von Edge zu Edge für alle Zweigstellen basierend auf den SLOs und der Anwendungsleistung her. Darüber hinaus bietet das Cloud-VPN eine sichere Verbindung über alle Zweigstellen hinweg mit PKI-skalierbarer Schlüsselverwaltung. Neue Zweigstellen treten automatisch dem VPN-Netzwerk bei und haben Zugriff auf alle Ressourcen in anderen Zweigstellen, Unternehmensdatencentern und Datencentern von Drittanbietern, wie Amazon AWS.

Eingehende QoS mit Mehrfachquelle

VMware SD-WAN klassifiziert mehr als 2.500 Anwendungen, die eine intelligente Steuerung ermöglichen. Die Standardeinstellungen legen die QoS-Parameter (Quality of Service) für verschiedene Anwendungstypen fest, wobei die IT nur zur Festlegung der Anwendungspriorität erforderlich ist. Die Kenntnis der Netzwerkanforderungen für verschiedene Anwendungstypen, automatische Link-Kapazitätsmessungen und dynamische Flussüberwachung ermöglichen die Automatisierung von QoS-Konfigurationen und Bandbreitenzuweisungen.

Firewall

VMware SD-WAN bietet eine zustands- und kontextorientierte (Anwendung, Benutzer, Gerät), integrierte anwendungsbezogene Firewall mit präziser Steuerung von Unteranwendungen, Unterstützung für Protokoll-Hopping-Anwendungen — wie Skype und andere Peer-to-Peer-Anwendungen (z. B. Skype-Video und Chat deaktivieren, Skype-Audio jedoch zulassen). Der sichere Firewalldienst ist benutzer- und gerätebetriebssystem-kompatibel mit der Möglichkeit, Sprach-, Video-, Daten- und Compliance-Verkehr zu trennen. Die Richtlinien für BYOD-Geräte (wie z. B. Apple iOS, Android, Windows und Mac OS) im Unternehmensnetzwerk lassen sich leicht steuern.

Einfügen von Netzwerkdiensten

Die VMware SD-WAN-Lösung unterstützt eine Plattform für das Hosting mehrerer virtualisierter Netzwerkfunktionen, um Einzelfunktions-Appliances zu eliminieren und die IT-Komplexität der Zweigstellen zu reduzieren. VMware SD-WAN-Dienstketten verbinden den Verkehr von der Zweigstelle zu den regionalen Cloud-basierten und Unternehmens-Hub-Diensten mit garantierter Leistung, Sicherheit und Verwaltbarkeit. Die Zweigstellen nutzen konsolidierte Sicherheits- und Netzwerkdienste, einschließlich derer von Partnern wie Zscaler und Websense. Mithilfe einer einfachen Schnittstelle können Dienste in die Cloud und lokal mit anwendungsspezifischen Richtlinien mit lediglich ein paar Klicks eingefügt werden.

Aktivierung

SD-WAN Edge-Appliances authentifizieren sich automatisch, stellen eine Verbindung her und erhalten Konfigurationsanweisungen, sobald sie mit dem Internet verbunden sind, und zwar in einer Zero-Touch-Bereitstellung. Sie liefern eine hochverfügbare Bereitstellung mit dem SD-WAN Edge-Redundanzprotokoll und integrieren sich in das bestehende Netzwerk mit Unterstützung des OSPF-Routing-Protokolls und profitieren von dynamischem Lernen und Automatisierung.

Overlay-Flow-Steuerung

Der SD-WAN Edge lernt Routen von benachbarten Routern über OSPF und BGP. Er sendet die gelernten Routen an das Gateway/den Controller. Das Gateway bzw. der Controller fungiert wie ein Routenreflektor und sendet die erlernten Routen an andere SD-WAN Edgess. Die OFC (Overlay Flow Control, Overlay-Flow-Steuerung) ermöglicht eine unternehmensweite Routensichtbarkeit und -steuerung für eine einfache Programmierung und für Voll- oder Teil-Overlay.

OSPF

VMware SD-WAN unterstützt Eingangs-/Ausgangsfilter zu OSPF-Nachbarn, OE1/OE2-Routentypen, MD5-Authentifizierung. Über OSPF gelernte Routen werden automatisch an den in der Cloud oder an die lokal gehosteten Controller weiterverteilt.

BGP

VMware SD-WAN unterstützt Eingangs-/Ausgangsfilter, und der Filter kann auf „Verweigern (Deny)“ festgelegt werden, oder optional kann das BGP-Attribut hinzugefügt/geändert werden, um die Pfadauswahl zu beeinflussen, d. h. „RFC 1998-Community (RFC 1998 community)“, „MED“, „AS-Pfad voranstellen (AS-Path prepend)“ und „Lokale Präferenz (local preference)“.

Segmentierung

Die Netzwerksegmentierung ist eine wichtige Funktion sowohl für Unternehmen als auch für Dienstanbieter. In der elementarsten Form bietet die Segmentierung eine Netzwerkisolierung aus Verwaltungs- und Sicherheitsgründen. Die gängigsten Formen der Segmentierung sind VLANs für L2 und VRFs für L3.

Typische Anwendungsfälle für die Segmentierung:

- Trennung der Geschäftsbereiche: Technik, HR usw. für Sicherheit/Audit
- Trennung von Benutzerdaten: Gast, PCI, Trennung des Unternehmensverkehrs
- Unternehmen verwendet überlappende IP-Adressen in verschiedenen VRFs

Der verwaltete Ansatz ist jedoch auf eine einzige Box oder zwei physisch verbundene Geräte beschränkt. Um die Funktionalität zu erweitern, müssen Segmentierungsinformationen über das Netzwerk übertragen werden.

VMware SD-WAN ermöglicht die durchgängige Segmentierung. Wenn das Paket den Edge durchläuft, wird die Segment-ID dem Paket hinzugefügt und an den Hub und das Cloud-Gateway weitergeleitet, wodurch eine Netzwerkdienstisolierung vom Edge zum Cloud und Datencenter ermöglicht wird. Dies bietet die Möglichkeit, Präfixe in einer eindeutigen Routing-Tabelle zu gruppieren und so die Unternehmensrichtline segmentierfähig zu machen.

Routing

Im dynamischen Routing lernt der SD-WAN Edge Routen von benachbarten Routern über OSPF oder BGP. Der SD-WAN Orchestrator verwaltet alle dynamisch erlernten Routen in einer globalen Routing-Tabelle mit dem Namen „Overlay-Flow-Steuerung“ (Overlay Flow Control). Die Overlay-Flow-Steuerung ermöglicht die Verwaltung dynamischer Routen im Fall von „Overlay-Flow-Steuerung-Synchronisierung“ und „Änderung der Konfiguration der Eingangs-/Ausgangsfilterung“. Die Änderung der Eingangsfilterung für ein Präfix von IGNORIEREN (IGNORE) auf LERNEN (LEARN) würde das Präfix aus der Overlay-Flow-Steuerung holen und in die Unified Routing-Tabelle installieren.

Weitere Informationen finden Sie unter Kapitel 19 Konfigurieren von dynamischem Routing mit OSPF oder BGP.

Unternehmensrichtlinien-Framework

Quality of Service (QoS), Ressourcenzuweisungen, Link/Pfad-Steuerung und Fehlerkorrektur werden automatisch auf der Grundlage von Unternehmensrichtlinien und Anwendungsprioritäten angewendet. Orchestrieren Sie den Verkehr auf der Grundlage von Transportgruppen, die durch private und öffentliche Links, Richtliniendefinition und Link-Merkmale definiert sind.

Tunnel-Overhead und MTU

VMware SD-WAN verursacht, wie jedes Overlay, zusätzlichen Overhead für den Datenverkehr, der das Netzwerk durchläuft. In diesem Abschnitt wird zunächst der in einem herkömmlichen IPsec-Netzwerk hinzugefügte Overhead und der Vergleich mit VMware SD-WAN beschrieben. Anschließend wird erläutert, wie sich dieser zusätzliche Overhead auf die MTU und das Verhalten der Paketfragmentierung im Netzwerk auswirkt.

IPsec-Tunnel-Overhead

In einem herkömmlichen IPSec-Netzwerk wird der Datenverkehr in der Regel in einem IPSec-Tunnel zwischen Endpoints übertragen. Ein Standard-IPsec-Tunnel-Szenario (AES 128-Bit-Verschlüsselung mit ESP [Encapsulating Security Payload]) führt bei der Verschlüsselung des Datenverkehrs wie folgt zu mehreren Arten von Overhead:

- **Auffüllung (Padding)**
  - AES verschlüsselt Daten in 16-Byte-Blöcken. Dies wird als Blockgröße bezeichnet.
  - Wenn der Hauptteil eines Pakets kleiner oder nicht durch die Blockgröße teilbar ist, wird er entsprechend der Blockgröße aufgefüllt.
  - Beispiele:
    - Aus einem 1-Byte-Paket werden 16 Byte mit einer Auffüllung von 15 Byte.
    - Aus einem 1400-Byte-Paket werden 1408 Byte mit einer Auffüllung von 8 Byte.
    - Für ein 64-Byte-Paket ist keine Auffüllung erforderlich.
- **IPsec-Header und -Trailer:**
  - UDP-Header für NAT Traversal (NAT-T).
  - IP-Header für IPSec-Tunnelmodus.
  - ESP-Header und -Trailer.

Element	Größe in Byte
UDP-Header	8
IP-Header	20
IPSec-Sequenznummer	4
IPSec SPI	4

Element	Größe in Byte
Initialisierungsvektor	16
Auffüllung	0 – 15
Auffüllungslänge	1
Nächste Kopfzeile	1
Authentifizierungsdaten	12
Gesamt	66 – 81

Hinweis Bei den angegebenen Beispielen wird davon ausgegangen, dass sich mindestens ein Gerät hinter einem NAT-Gerät befindet. Wenn kein NAT verwendet wird, ist der IPSec-Overhead um 20 Byte geringer, da NAT-T nicht benötigt wird. Es gibt keine Änderung am Verhalten von VMware SD-WAN, unabhängig davon, ob NAT vorhanden ist oder nicht (NAT-T ist immer aktiviert).

VMware SD-WAN-Tunnel-Overhead

Zur Unterstützung von Dynamic Multipath Optimization™ (DMPO) kapselt VMware SD-WAN Pakete in einem Protokoll namens VeloCloud Multipath Protocol (VCMP). VCMP fügt 31 Byte Overhead für Benutzerpakete hinzu, um Resequenzierung, Fehlerkorrektur, Netzwerkanalyse und Netzwerksegmentierung innerhalb eines einzelnen Tunnels zu unterstützen. VCMP wird auf dem von der IANA registrierten Port UDP 2426 verwendet. Um ein konsistentes Verhalten in allen möglichen Szenarien zu gewährleisten (unverschlüsselt, verschlüsselt und hinter einem NAT, verschlüsselt aber nicht hinter einem NAT), wird VCMP mit dem Transportmodus IPsec verschlüsselt und erzwingt, dass NAT-T mit dem speziellen NAT-T-Port 2426 „True“ ist.

Pakete, die über das SD-WAN Gateway an das Internet gesendet werden, werden standardmäßig nicht verschlüsselt, da sie bei Verlassen des Gateways ins offene Internet gelangen. Dies hat zur Folge, dass der Overhead für Internet-Multipath-Datenverkehr geringer ist als der VPN-Datenverkehr.

Hinweis Dienstanbieter haben die Möglichkeit, den Internetdatenverkehr über das Gateway zu verschlüsseln. Wenn sie diese Option verwenden, gilt der VPN-Overhead auch für den Internetdatenverkehr.

VPN-Datenverkehr

Element	Größe in Byte
UDP-Header	8
IP-Header	20
IPSec-Sequenznummer	4
IPSec SPI	4
VCMP-Header	23

Element	Größe in Byte
VCMP-Datenheader	8
Initialisierungsvektor	16
Auffüllung	0 – 15
Auffüllungslänge	1
Nächste Kopfzeile	1
Authentifizierungsdaten	12
Gesamt	97 – 112

Internet-Multipath-Datenverkehr

Element	Größe in Byte
UDP-Header	8
IP-Header	20
VCMP-Header	23
VCMP-Datenheader	8
Gesamt	59

Path MTU Discovery

Nachdem ermittelt wurde, wie viel Overhead angewendet wird, muss der SD-WAN Edge die maximal zulässige MTU ermitteln, um die effektive MTU für Kundenpakete zu berechnen. Um die maximal zulässige MTU zu ermitteln, führt der Edge Path MTU Discovery aus:

- Für öffentliche Internet-WAN-Verbindungen:
  - Path MTU Discovery wird für alle Gateways ausgeführt.
  - Die MTU für alle Tunnel wird auf die erkannte Mindest-MTU festgelegt.
- Für private WAN-Verbindungen:
  - Path MTU Discovery wird für alle anderen Edges im Kundennetzwerk durchgeführt.
  - Die MTU für jeden Tunnel wird basierend auf den Ergebnissen von Path MTU Discovery festgelegt.

Der Edge versucht zunächst eine RFC 1191 Path MTU-Erkennung, bei der ein Paket der aktuellen bekannten Link-MTU (Standard: 1500 Byte) an den Peer gesendet wird, wobei das „Don't Fragment“-Bit (DF) im IP-Header gesetzt ist. Wenn dieses Paket auf dem Remote-Edge oder Gateway empfangen wird, wird ein Bestätigungspaket derselben Größe an den Edge zurückgegeben. Wenn das Paket den Remote-Edge oder das Gateway aufgrund der Einschränkungen der MTU nicht erreichen kann, wird erwartet, dass das Zwischengerät eine

Meldung über ein nicht erreichbares (Fragmentierung erforderlich) ICMP-Ziel sendet. Wenn der Edge die ICMP-Unerreichbarkeitsmeldung erhält, wird die Meldung validiert (um sicherzustellen, dass der gemeldete MTU-Wert vernünftig ist). Nach der Validierung wird die MTU angepasst. Der Vorgang wird dann wiederholt, bis die MTU erkannt wurde.

In einigen Fällen (z. B. bei USB-LTE-Dongles) sendet das Zwischengerät keine ICMP-Unerreichbarkeitsnachricht, selbst wenn das Paket zu groß ist. Wenn RFC 1191 fehlschlägt (der Edge hat keine Bestätigung erhalten, oder ICMP ist nicht erreichbar), wird auf RFC 4821 Packetization Layer Path MTU Discovery zurückgegriffen. Der Edge versucht, eine binäre Suche auszuführen, um die MTU zu ermitteln.

Wenn eine MTU für einen Peer erkannt wird, werden alle Tunnel zu diesem Peer auf dieselbe MTU festgelegt. Das heißt, wenn ein Edge eine Verbindung mit einer MTU von 1400 Byte und eine Verbindung mit einer MTU von 1500 Byte hat, haben alle Tunnel eine MTU von 1400 Byte. Dadurch wird sichergestellt, dass Pakete jederzeit mit derselben MTU auf einem beliebigen Tunnel gesendet werden können. Diese wird als **effektive Edge-MTU** bezeichnet. Basierend auf dem Ziel (VPN oder Internet Multipath) wird der oben umrissene Overhead subtrahiert, um die **effektive Paket-MTU** zu berechnen. Für direktes Internet oder sonstigen zugrunde liegenden Datenverkehr ist der Overhead 0 Byte. Da kein Failover der Verbindung erforderlich ist, ist die effektive Paket-MTU identisch mit der erkannten WAN-Verbindungs-MTU.

Hinweis VMware SD-WAN RFC 4821 Packetization Layer Path MTU Discovery misst die MTU bis zu einem Minimum von 1300 Byte. Wenn Ihre MTU kleiner als 1300 Byte ist, müssen Sie die MTU manuell konfigurieren.

VPN-Datenverkehr und MTU

Nachdem der SD-WAN Edge die MTU und die Overheads ermittelt hat, kann eine effektive MTU für den Clientdatenverkehr berechnet werden. Der Edge versucht, diese MTU so effizient wie möglich für die verschiedenen potenziellen Arten von empfangenem Datenverkehr durchzusetzen.

TCP-Datenverkehr

Der Edge führt die TCP MSS-Anpassung (Maximum Segment Size) für empfangene TCP-Pakete automatisch durch. Während SYN- und SYN|ACK-Pakete den Edge durchlaufen, wird die MSS auf der Grundlage der effektiven Paket-MTU neu geschrieben.

Kein TCP-Datenverkehr ohne gesetztes DF-Bit

Wenn das Paket größer ist als die effektive Paket-MTU, führt der Edge automatisch die IP-Fragmentierung gemäß RFC 791 durch.

Kein TCP-Datenverkehr mit gesetztem DF-Bit

Wenn das Paket größer ist als die effektive Paket-MTU:

- Wenn ein Paket zum ersten Mal für diesen Flow (IP 5-Tupel) empfangen wird, verwirft der Edge das Paket und sendet eine Meldung über ein nicht erreichbares (Fragmentierung erforderlich) ICMP-Ziel gemäß RFC 791.

- Wenn nachfolgende Pakete für denselben Flow empfangen werden, die immer noch zu groß sind, werden diese Pakete in mehrere VCMP-Pakete fragmentiert und vor der Übergabe an das Remote-Ende transparent neu zusammengesetzt.

Netzwerktopologien

In diesem Abschnitt werden Netzwerktopologien für Zweigstellen und Datencenter beschrieben.

Verzweigungen zu privaten Drittanbietern (VPN)

Kunden mit einem privaten Datencenter oder einem Datencenter in der Cloud wünschen sich häufig eine Möglichkeit, dies in ihr Netzwerk aufzunehmen, ohne einen Tunnel von jeder einzelnen Zweigstelle zum Datencenter definieren zu müssen. Indem Sie die Site als eine Non VMware SD-WAN Site definieren, wird ein einzelner Tunnel vom nächstgelegenen SD-WAN Gateway zum vorhandenen Router oder zur virtuellen Firewall des Kunden aufgebaut. Alle SD-WAN Edges-Instanzen, die mit der Site kommunizieren müssen, stellen eine Verbindung mit demselben SD-WAN Gateway her, um Pakete über den Tunnel weiterzuleiten, und vereinfachen so die gesamte Netzwerkkonfiguration und Einrichtung der neuen Site.

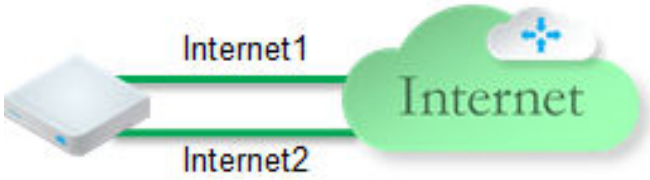
VMware SD-WAN vereinfacht die Bereitstellung der Zweigstelle und liefert dem Unternehmen eine hervorragende Anwendungsleistung oder eine öffentliche/private Verbindung für Cloud- und/oder lokale Anwendungen.

Topologien der Zweigstellen-Site

Der VMware SD-WAN-Dienst definiert zwei oder mehr unterschiedliche Zweigstellentopologien, die als Bronze, Silver und Gold bezeichnet sind. Darüber hinaus können SD-WAN Edges-Paare in einer Hochverfügbarkeitskonfiguration (HA-Konfiguration) an einem Zweigstellenstandort konfiguriert werden.

Topologie der Bronze-Site

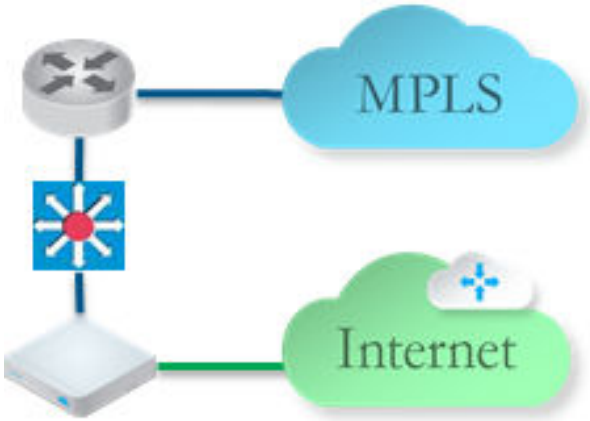
Die Bronze-Topologie stellt die typische Bereitstellung einer kleinen Site dar, bei der ein oder zwei WAN-Links mit dem öffentlichen Internet verbunden sind. In der Bronze-Topologie gibt es keine MPLS-Verbindung, und es gibt keinen L3-Switch auf der LAN-Seite des SD-WAN Edge. Die folgende Abbildung zeigt eine Übersicht über die Bronze-Topologie.



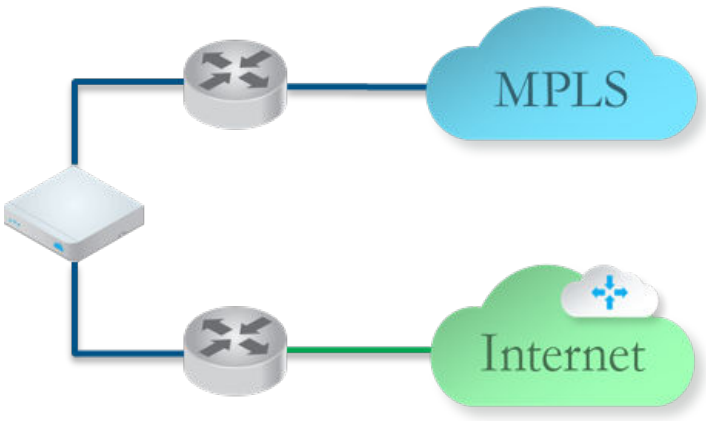
Topologie der Silver-Site

Die Silver-Topologie stellt eine Site dar, die neben einem oder mehreren öffentlichen Internet-Links auch über eine MPLS-Verbindung verfügt. Es gibt zwei Varianten dieser Topologie.

Bei der ersten Variante handelt es sich um einen einzelnen L3-Switch mit einem oder mehreren öffentlichen Internet-Links und einem MPLS-Link, der auf einem CE beendet wird und über den L3-Switch zugänglich ist. In diesem Fall wird der SD-WAN Edge zwischen dem L3-Switch und dem Internet geschaltet (und ersetzt die vorhandene Firewall/Router).

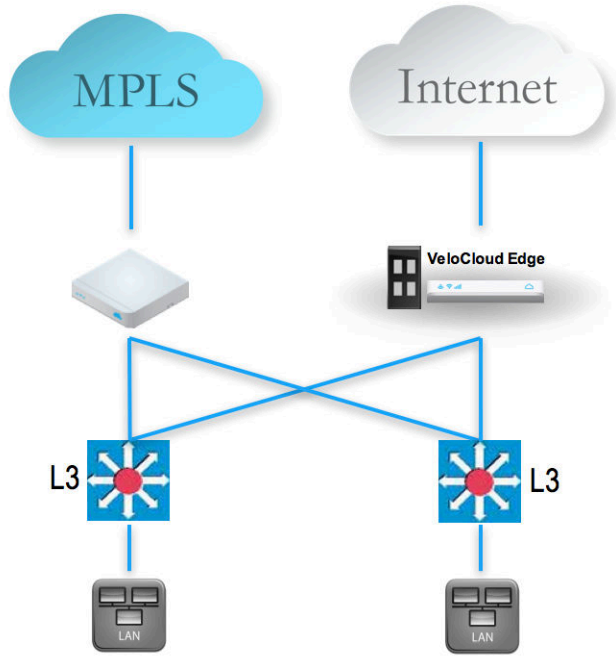


Die zweite Variante umfasst MPLS und Internet-Router, die unter Verwendung von HSRP mit einem L2-Switch auf der LAN-Seite eingesetzt werden. In diesem Fällen ersetzt der SD-WAN Edge den L2-Switch.

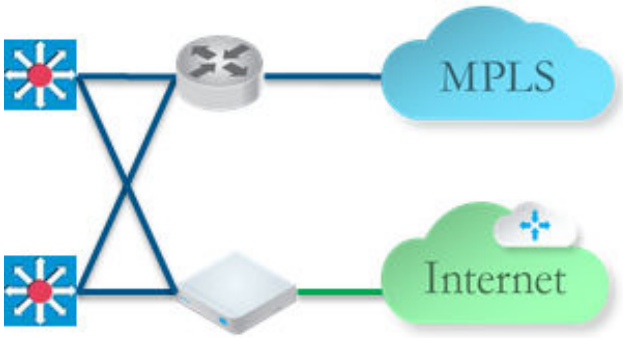


Topologie der Gold-Site

Die Gold-Topologie ist eine typische Topologie für große Zweigstellen-Sites. Die Topologie umfasst L3-Switches (aktiv/aktiv), die Routen über OSPF oder BGP übermitteln, einen oder mehrere öffentliche Internet-Links und einen MPLS-Link, der auf einem CE-Router endet, der ebenfalls mit OSPF oder BGP kommuniziert und über die L3-Switches zugänglich ist.

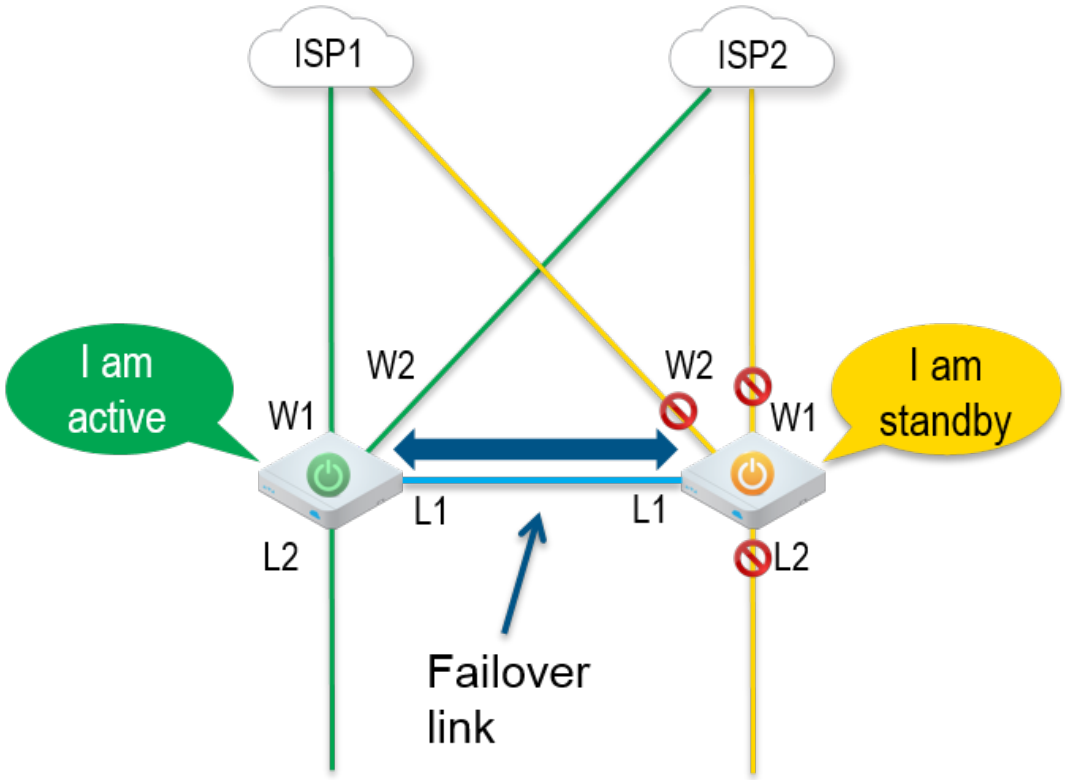


Ein wichtiger Unterscheidungspunkt ist dabei, dass ein einziger WAN-Link über zwei geroutete Schnittstellen zugänglich ist. Um dies zu unterstützen, wird eine virtuelle IP-Adresse innerhalb des Edge bereitgestellt, die über OSPF oder BGP angekündigt oder statisch an die Schnittstellen weitergeleitet werden kann.



High Availability (HA)-Konfiguration

Die folgende Abbildung bietet eine konzeptionelle Übersicht über die VMware SD-WAN-Hochverfügbarkeitskonfiguration mit zwei SD-WAN Edges-Instanzen, einem aktiven und einem Standby-Edge.



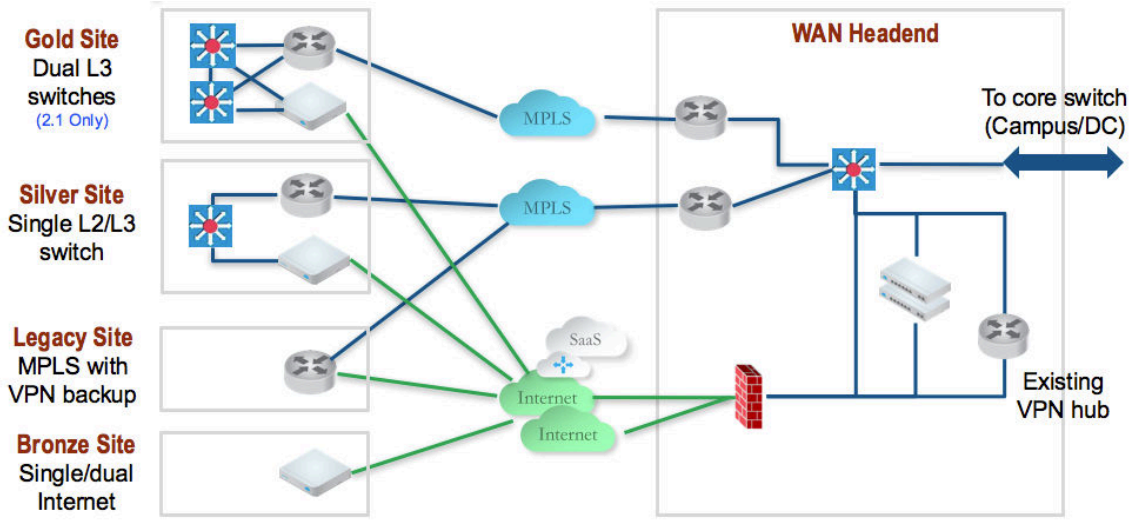
Die Verbindung der L1-Ports an jedem Edge dient zum Erstellen eines Failover-Links. Der Standby-SD-WAN Edge blockiert alle Ports mit Ausnahme des L1-Ports für den Failover-Link.

Lokale Topologie

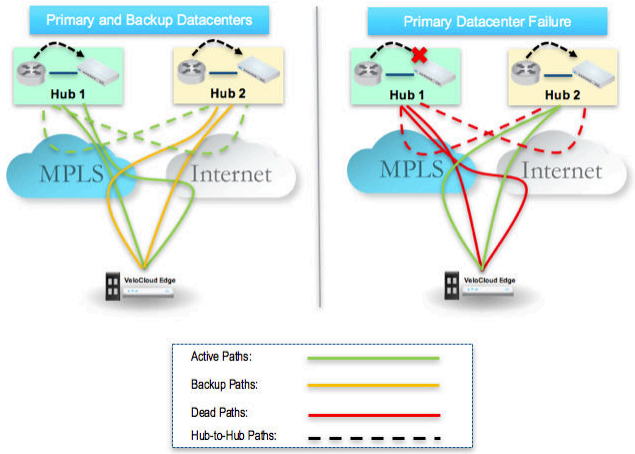
Die lokale Topologie besteht aus zwei Hubs und mehreren Zweigstellen, mit oder ohne SD-WAN Edge. Jeder Hub verfügt über eine hybride WAN-Konnektivität. Es gibt mehrere Zweigstellen-Typen.

Hinweis Die Gold-Site ist derzeit nicht Gegenstand dieser Version und wird zu einem späteren Zeitpunkt hinzugefügt.

Im MPLS-Netzwerk werden BGP und Peers mit allen CE-Routern ausgeführt. Auf Hub-1-, Hub-2- und Silver-1-Sites führt der L3-Switch OSPF oder BGP mit dem CE-Router und der Firewall (im Falle von Hub-Sites) aus.



In einigen Fällen kann es vorkommen, dass redundante Datencenter vorhanden sind, die die gleichen Subnetze mit unterschiedlichen Kosten ankündigen. In diesem Szenario können beide Datencenter als Edge-zu-Edge-VPN-Hubs konfiguriert werden. Da alle Edges direkt mit jedem Hub verbunden sind, sind die Hubs tatsächlich auch direkt miteinander verbunden. Basierend auf den Routenkosten wird der Datenverkehr an das bevorzugte aktive Datencenter geleitet.



In früheren Versionen konnten Benutzer ein Unternehmensobjekt mithilfe von Zscaler oder Palo Alto Network als generische Non VMware SD-WAN Site erstellen. In Version 2.0 ist dieses Objekt jetzt die Non VMware SD-WAN Site erster Wahl.

Die Cloud-Lösung von VMware SD-WAN kombiniert die Wirtschaftlichkeit und Flexibilität des hybriden WAN mit der Bereitstellungsgeschwindigkeit und dem geringen Wartungsaufwand von cloudbasierten Diensten. Sie stellt virtualisierte Dienste aus der Cloud für Zweigstellen bereit und vereinfacht so das WAN erheblich. Die Ausrüstung für den Kundenstandort von VMware SD-WAN, die SD-WAN Edge, aggregiert mehrere Breitband-Links (z. B. Kabel, DSL, 4G-LTE) in der Zweigstelle und sendet den Datenverkehr an SD-WAN Gateways. Durch cloudbasierte Orchestrierung kann der Dienst die Zweigstelle mit jeder Art von Datencenter verbinden: Unternehmen, Cloud oder Software-as-a-Service.

SD-WAN Edge ist ein kompaktes, schlankes Thin-Edge-Gerät, das für eine sichere, optimierte Konnektivität mit Anwendungen und Daten aus der Cloud heraus ohne Mitwirkung von IT-Experten bereitgestellt wird. Ein Cluster von Gateways wird weltweit in erstklassigen Cloud-Datencentern eingesetzt, um skalierbare und bedarfsorientierte Cloud-Netzwerkdienste bereitzustellen. Bei der Arbeit mit dem Edge bietet der Cluster eine dynamische Mehrfachpfadoptimierung, sodass mehrere gewöhnliche Breitbandverbindungen als eine einzige Verbindung mit hoher Bandbreite erscheinen. Die Orchestrator-Verwaltung bietet eine zentralisierte Konfiguration, Echtzeit-Überwachung und die Bereitstellung virtueller Dienste mit einem Klick.

Rollen und Berechtigungsstufen

VMware SD-WAN verfügt über vordefinierte Rollen mit unterschiedlichen Rechten.

- IT-Administratoren (oder Administrator)
- Site-Kontakt auf jeder Site, auf der ein SD-WAN Edge-Gerät bereitgestellt wird
- IT-Operator (oder Operator)
- IT-Partner (oder Partner)

Administrator

Der Administrator konfiguriert, überwacht und verwaltet den VMware SD-WAN-Dienstbetrieb. Es sind drei Administratorrollen vorhanden:

Administratorrolle	Beschreibung
Enterprise-Standard-Administrator	Kann alle Konfigurations- und Überwachungsaufgaben ausführen.
Enterprise-Superuser	Kann die gleichen Aufgaben wie ein Enterprise-Standard-Administrator ausführen und darüber hinaus zusätzliche Benutzer mit den Rollen „Enterprise-Standard-Administrator“, „Enterprise-MSP“ und „Kundensupport“ erstellen.
Enterprise-Support	Kann Konfigurationsüberprüfungs- und Überwachungsaufgaben ausführen, aber keine Anwendungsstatistiken mit identifizierbaren Informationen von Benutzern anzeigen, und kann nur Konfigurationsinformationen anzeigen.

Hinweis Ein Administrator sollte eingehend mit Netzwerkkonzepten, Webanwendungen sowie Anforderungen und Verfahren für das Unternehmen vertraut sein.

Site-Kontakt

Der **Site-Kontakt (Site Contact)** ist verantwortlich für die physische Installation und Aktivierung des SD-WAN Edge mit dem VMware SD-WAN-Dienst. Der Site-Kontakt ist eine nicht im IT-Bereich tätige Person, die die Möglichkeit hat, eine E-Mail zu erhalten und die Anweisungen in der E-Mail für die Edge-Aktivierung auszuführen.

Operator

Der Operator kann alle Aufgaben ausführen, die ein Administrator ausführen kann, sowie zusätzliche operatorspezifische Aufgaben – z. B. Erstellen und Verwalten von Kunden, Cloud-Edges und Gateways. Es sind vier Operatorrollen vorhanden:

Operatorrolle	Beschreibung
Standard-Operator	Kann alle Konfigurations- und Überwachungsaufgaben ausführen.
Superuser-Operator	Kann zusätzliche Benutzer mit den Operatorrollen anzeigen und erstellen.
Business-Specialist-Operator	Kann Kundenkonten erstellen und verwalten.
Kundensupport-Operator	Kann Edges und Aktivität überwachen.

Ein Operator sollte eingehend mit Netzwerkkonzepten, Webanwendungen sowie Anforderungen und Verfahren für das Unternehmen vertraut sein.

Partner

Der **Partner** kann alle Aufgaben ausführen, die ein Administrator ausführen kann, sowie weitere partnerspezifische Aufgaben – z. B. Erstellen und Verwalten von Kunden. Es sind vier Partnerrollen vorhanden:

Partnerrolle	Beschreibung
Standard-Administrator	Kann alle Konfigurations- und Überwachungsaufgaben ausführen.
Superuser	Kann zusätzliche Benutzer mit den Partnerrollen anzeigen und erstellen.
Business-Specialist	Kann Konfigurations- und Überwachungsaufgaben durchführen, aber keine Anwendungsstatistiken mit identifizierbaren Informationen von Benutzern anzeigen.
Kundensupport	Kann Konfigurationsüberprüfungs- und Überwachungsaufgaben ausführen, aber keine Anwendungsstatistiken mit identifizierbaren Informationen von Benutzern anzeigen, und kann nur Konfigurationsinformationen anzeigen.

Ein Partner sollte eingehend mit Netzwerkkonzepten, Webanwendungen sowie Anforderungen und Verfahren für das Unternehmen vertraut sein.

Benutzerrollenmatrix

In diesem Abschnitt wird der Funktionsumfang gemäß VMware SD-WAN-Benutzerrollen beschrieben.

SD-WAN Orchestrator-Funktionen auf Operator-Ebene – Benutzerrollenmatrix

In der folgenden Tabelle werden die Benutzerrollen auf Operator-Ebene aufgeführt, die Zugriff auf die SD-WAN Orchestrator-Funktionen haben.

- R: Lesen
- W: Schreiben (Ändern/Bearbeiten)

- D: Löschen
- NA: Kein Zugriff

SD-WAN Orchestrator-Funktion	Operator: Superuser-Operator	Operator: Standard-Operator	Partner: Business-Specialist	Partner: Kundensupport-Operator	Superuser	Standard-Administrator	Business-Specialist	Kundens
Überwachen von Kunden	R	R	R	R	R	R	R	R
Verwalten von Kunden	RWD	RWD	RWD	R	RWD	RWD	RWD	R
Verwalten von Partnern	RWD	RWD	RWD	R	NA	NA	NA	NA
(Verwalten des Edge) Software-Images	RWD	RWD	R	R	*Siehe Hinweis	*Siehe Hinweis	*Siehe Hinweis	*Siehe H
Systemeigenschaften	RWD	R	NA	R	NA	NA	NA	NA
Operator-Ereignisse	R	R	NA	R	NA	NA	NA	NA
Operator-Profile	RWD	RWD	R	R	NA	NA	NA	NA
Operator-Benutzer	RWD	R	R	R	NA	NA	NA	NA
Gateway-Pools	RWD	RW	R	R	RWD	RWD	NA	R
Gateways	RWD	RWD	R	R	RW	RW	NA	R
Gateway-Diagnosepakete	RWD	RWD	R	R	NA	NA	NA	NA
Anwendungszuordnungen	RWD	RWD	R	R	NA	NA	NA	NA
CA-Zusammenfassung	RW	R	R	R	NA	NA	NA	NA
Orchestrator-Authentifizierung	RWD	R	NA	R	NA	NA	NA	NA
Replizierung	RW	R	NA	R	NA	NA	NA	NA

Hinweis Operator-Superuser haben „RWD“-Zugriff auf zertifikatbezogene Konfigurationen, und Standard-Operatoren haben schreibgeschützten Zugriff auf zertifikatbezogene Konfigurationen. Diese Benutzer können über den Navigationsbereich unter **Konfigurieren (Configure) > Edges** auf die zertifikatbezogenen Konfigurationen zugreifen.*

Hinweis Enterprise-Benutzer auf allen Ebenen haben keinen Zugriff auf die Funktionen der Operator-Ebene.

SD-WAN Orchestrator-Funktionen auf Partnerebene – Benutzerrollenmatrix

In der folgenden Tabelle werden die Benutzerrollen auf Partnerebene aufgeführt, die Zugriff auf die SD-WAN Orchestrator-Funktionen haben.

- R: Lesen
- W: Schreiben (Ändern/Bearbeiten)
- D: Löschen

- NA: Kein Zugriff

SD-WAN Orchestrator-Funktion	Partner: Superuser	Partner: Standard-Administrator	Business-Specialist	Kundensupport
Überwachen von Kunden	R	R	R	R
Verwalten von Kunden	RWD	RWD	RWD	R
Ereignisse	R	R	NA	R
Admins	RWD	R	NA	R
Übersicht	R	R	R	R
Einstellungen	RW	R	R	R
Gateway-Pools	RW	RWD	NA	R
Gateways	RW	RW	NA	R

SD-WAN Orchestrator-Funktionen auf Unternehmensebene – Benutzerrollenmatrix

In der folgenden Tabelle werden die Benutzerrollen auf Enterprise-Ebene aufgeführt, die Zugriff auf die SD-WAN Orchestrator-Funktionen haben.

- R: Lesen
- W: Schreiben (Ändern/Bearbeiten)
- D: Löschen
- NA: Kein Zugriff

SD-WAN Orchestrator-Funktion	Enterprise: Superuser	Enterprise: Standard-Administrator	Kundensupport	Nur Lesen
Überwachen (Monitor) > Edges	R	R	R	R
Überwachen (Monitor) > Netzwerkdienste (Network Services)	R	R	R	R
Überwachen (Monitor) > Routing	R	R	R	NA
Überwachen (Monitor) > Warnungen (Alerts)	R	R	R	NA
Überwachen (Monitor) > Ereignisse (Events)	R	R	R	NA
Konfigurieren (Configure) > Edges	RWD	RWD	R	NA
Konfigurieren (Configure) > Profile (Profiles)	RWD	RWD	R	NA
Konfigurieren (Configure) > Netzwerke (Networks)	RWD	RWD	R	NA
Konfigurieren (Configure) > Segmente (Segments)	RWD	RWD	R	NA
Konfigurieren (Configure) > Overlay-Flow-Steuerung (Overlay Flow Control)	RWD	RWD	R	NA

SD-WAN Orchestrator-Funktion	Enterprise: Superuser	Enterprise: Standard-Administrator	Kundensupport	Nur Lesen
Konfigurieren (Configure) > Netzwerkdienste (Network Services)	RWD	RWD	R	NA
Konfigurieren (Configure) > Warnungen und Benachrichtigungen (Alerts & Notifications)	RW	RW	R	NA
Testen und Fehlerbehebung (Test & Troubleshoot) > Remote-Diagnose (Remote Diagnostics)	RW	RW	RW	NA
Testen und Fehlerbehebung (Test & Troubleshoot) > Remote-Aktionen (Remote Actions)	RW	RW	RW	NA
Testen und Fehlerbehebung (Test & Troubleshoot) > Paketerfassung (Packet Capture)	RW	RW	RW	NA
Verwaltung (Administration) > Systemeinstellungen (System Settings)	RW	RW	RW	NA
Verwaltung (Administration) > Administratoren (Administrators)	RW	R	R	NA

Hinweis Operator-Benutzer haben vollständigen Zugriff auf die SD-WAN Orchestrator-Funktionen.

Wichtige Konzepte

In diesem Abschnitt werden die wichtigen Konzepte und die wesentlichen Konfigurationseinstellungen von SD-WAN Orchestrator erläutert.

Konfigurationen

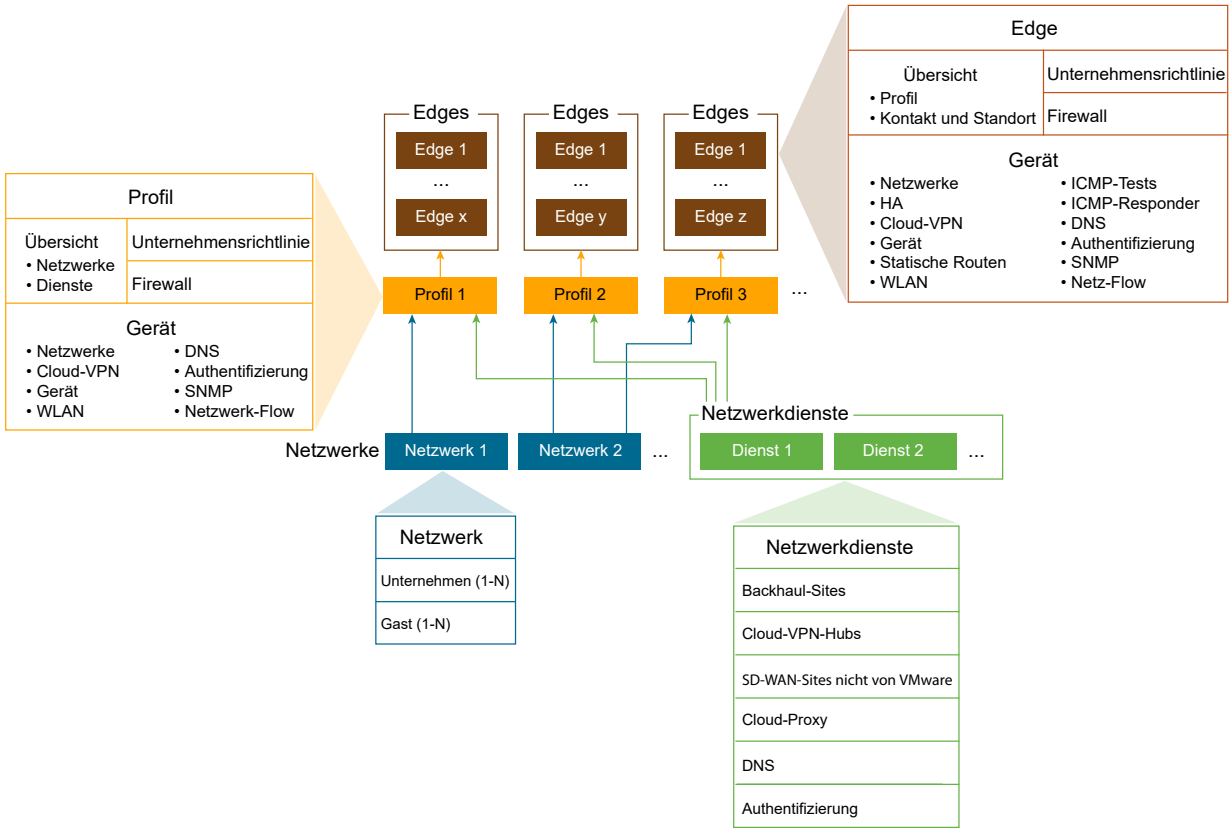
Der VMware SD-WAN-Dienst verfügt über vier Kernkonfigurationen, die eine hierarchische Beziehung aufweisen. Erstellen Sie diese Konfigurationen in SD-WAN Orchestrator.

Die folgende Tabelle bietet einen Überblick über die Konfigurationen.

Konfiguration	Beschreibung
Netzwerk	Definiert grundlegende Netzwerkkonfigurationen, wie z. B. IP-Adressierung und VLANs. Netzwerke können als „Unternehmen“ oder „Gast“ bezeichnet werden. Außerdem kann es für jedes Netzwerk mehrere Definitionen geben.
Netzwerkdienste	Definieren Sie mehrere gängige Dienste, die vom VMware SD-WAN-Dienst verwendet werden, wie z. B. BackHaul-Sites, Cloud-VPN-Hubs, Non VMware SD-WAN Sites-Instanzen, Cloud-Proxy-Dienste, DNS-Dienste und Authentifizierungsdienste.

Konfiguration	Beschreibung
Profil	Definiert eine Vorlagenkonfiguration, die auf mehrere Edges angewendet werden kann. Ein Profil wird konfiguriert, indem eine Netzwerk und Netzwerkdienste ausgewählt werden. Ein Profil kann auf ein oder mehrere Edge-Modelle angewendet werden und definiert die Einstellungen für LAN-, Internet-, WLAN- und WAN-Edge-Schnittstellen. In Profilen können auch Einstellungen für WLAN-Funk, SNMP, NetFlow, Unternehmensrichtlinien und die Firewallkonfiguration bereitgestellt werden.
Edge	Konfigurationen bieten einen vollständigen Satz an Einstellungen, die auf ein Edge-Gerät heruntergeladen werden können. Bei der Edge-Konfiguration handelt es sich um mehrere Einstellungen aus einem ausgewählten Profil, einem ausgewählten Netzwerk oder aus Netzwerkdiensten. Eine Edge-Konfiguration kann auch Einstellungen außer Kraft setzen oder fügt sortierte Richtlinien zu den im Profil, im Netzwerk und in den Netzwerkdiensten definierten Richtlinien hinzu.

Die folgende Abbildung bietet einen detaillierten Überblick über die Beziehungen und Konfigurationseinstellungen mehrerer Edges, Profile, Netzwerke und Netzwerkdienste.



Ein einzelnes Profil kann mehreren Edges zugewiesen werden. Eine einzelne Netzwerkkonfiguration kann in mehreren Profilen verwendet werden. Konfigurationen von Netzwerkdiensten werden in allen Profilen verwendet.

Netzwerke (Networks)

Bei Netzwerken handelt es sich um Standardkonfigurationen, die Netzwerkadressbereiche und VLAN-Zuweisungen für Edges definieren. Sie können die folgenden Netzwerktypen konfigurieren:

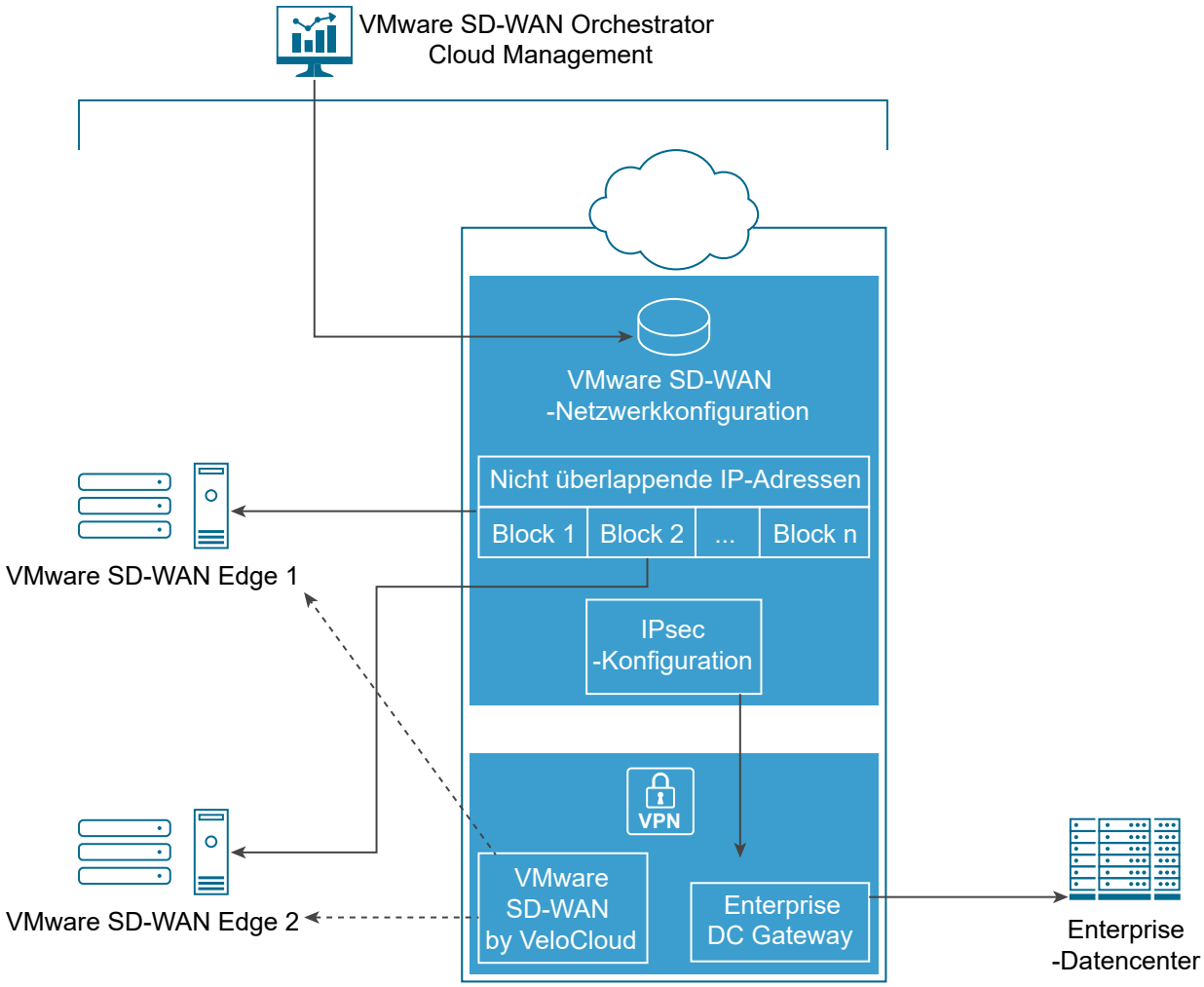
- Unternehmensnetzwerke oder vertrauenswürdige Netzwerke, die entweder mit überlappenden oder nicht überlappenden Adressen konfiguriert werden können.
- Gastnetzwerke oder nicht vertrauenswürdige Netzwerke, die immer überlappende Adressen verwenden.

Sie können mehrere Unternehmens- und Gastnetzwerke definieren und beiden Netzwerken VLANs zuweisen.

Bei überlappenden Adressen weisen alle Edges, die das Netzwerk verwenden, denselben Adressbereich auf. Überlappende Adressen sind mit Nicht-VPN-Konfigurationen verknüpft.

Bei nicht überlappenden Adressen wird ein Adressraum in Blöcke mit einer gleichen Anzahl von Adressen aufgeteilt. Nicht überlappende Adressen sind mit VPN-Konfigurationen verknüpft. Die Adressblöcke werden den Edges zugewiesen, die das Netzwerk verwenden, sodass jeder Edge über einen eindeutigen Satz an Adressen verfügt. Nicht überlappende Adressen werden für **Edge-zu-Edge**- und **Edge -zu-** Non VMware SD-WAN Site-VPN-Kommunikation benötigt. Die VMware SD-WAN-Konfiguration erstellt die erforderlichen Informationen, um auf ein Enterprise Data Center-Gateway für den VPN-Zugriff zuzugreifen. Ein Administrator für das Enterprise Data Center-Gateway verwendet die IPSec-Konfigurationsinformationen, die während der Konfiguration des Non VMware SD-WAN Site-VPN generiert wurden, zum Konfigurieren des Tunnels zur Non VMware SD-WAN Site.

In der folgenden Abbildung wird die Zuweisung eindeutiger IP-Adressblöcke aus einer Netzwerkkonfiguration zu SD-WAN Edges dargestellt.



Hinweis Wenn Sie nicht überlappende Adressen verwenden, teilt der SD-WAN Orchestrator automatisch den Edges die Adressblöcke zu. Die Zuteilung erfolgt basierend auf der maximalen Anzahl der Edges, die ggf. die Netzwerkkonfiguration nutzen.

Netzwerkdienste

Sie können Ihre Unternehmensnetzwerkdienste definieren und für alle Profile verwenden. Hierzu gehören Dienste für Authentifizierung, Cloud-Proxy, Non VMware SD-WAN Sites-Instanzen und DNS. Die definierten Netzwerkdienste werden nur dann verwendet, wenn sie einem Profil zugewiesen sind.

Profile

Bei einem Profil handelt es sich um eine benannte Konfiguration, durch die eine Liste von VLANs, Cloud-VPN-Einstellungen, kabelgebundenen und Wireless-Schnittstelleneinstellungen sowie Netzwerkdiensten wie DNS-Einstellungen, Authentifizierungseinstellungen, Cloud-Proxy-Einstellungen und VPN-Verbindungen mit Non VMware SD-WAN Sites definiert wird. Mithilfe der Profile können Sie eine Standardkonfiguration für einen oder mehrere SD-WAN Edgess definieren.

Profile enthalten Cloud-VPN-Einstellungen für Edges, die für VPN konfiguriert sind. Mit den Cloud-VPN-Einstellungen können Edge-zu-Edge- und Edge-zu-Non VMware SD-WAN Site-VPN-Verbindungen aktiviert oder deaktiviert werden.

Darüber hinaus können in Profilen Regeln und Konfigurationen für Unternehmensrichtlinien und Firewalleinstellungen definiert werden.

Edges

Sie können einem Edge ein Profil zuweisen. Der Edge leitet den größten Teil der Konfigurationseinstellungen aus dem Profil ab.

Die meisten in einem Profil oder Netzwerk oder in Netzwerkdiensten definierten Einstellungen können Sie ohne Änderung in einer Edge-Konfiguration verwenden. Sie können die Einstellungen für die Edge-Konfigurationselemente jedoch auch außer Kraft setzen, um einen Edge für ein bestimmtes Szenario anzupassen. Hierzu gehören Einstellungen für Schnittstellen, WLAN-Funk, DNS, Authentifizierung, Unternehmensrichtlinien und Firewalls.

Darüber hinaus können Sie einen Edge so konfigurieren, dass er um Einstellungen ergänzt wird, die in der Profil- oder Netzwerkkonfiguration nicht vorhanden sind. Hierzu gehören Subnetzadressierung, Einstellungen für statische Routen und eingehende Firewallregeln für Portweiterleitung und 1:1-NAT.

Workflow für die Orchestrator-Konfiguration

VMware SD-WAN unterstützt mehrere Konfigurationsszenarien. In der folgenden Tabelle sind einige der gängigen Szenarien aufgelistet:

Szenario	Beschreibung
SaaS	Wird für Edges verwendet, die keine VPN-Verbindungen zwischen Edges zu einer Non VMware SD-WAN Site oder einer VMware SD-WAN Site benötigen. Im Workflow wird davon ausgegangen, dass bei der Adressierung für das Unternehmensnetzwerk überlappende Adressen verwendet werden.
Non VMware SD-WAN Site über VPN	Wird für Edges verwendet, die VPN-Verbindungen mit einer Non VMware SD-WAN Site benötigen, wie z. B. Amazon Web Services, Zscaler, Cisco ISR oder die ASR 1000-Serie. In diesem Workflow wird davon ausgegangen, dass bei der Adressierung für das Unternehmensnetzwerk nicht überlappende Adressen und die Non VMware SD-WAN Sites im Profil definiert sind.
VMware SD-WAN Site-VPN	Wird für Edges verwendet, die VPN-Verbindungen mit einer VMware SD-WAN Site benötigen, wie z. B. Edge- oder Cloud-VPN-Hub. In diesem Workflow wird davon ausgegangen, dass bei der Adressierung für das Unternehmensnetzwerk nicht überlappende Adressen und die VMware SD-WAN Sites im Profil definiert sind.

Führen Sie für jedes Szenario die Konfigurationen im SD-WAN Orchestrator in der nachstehenden Reihenfolge durch:

Schritt 1: Netzwerk

Schritt 2: Netzwerkdienste

Schritt 3: Profil

Schritt 4: Edge

In der folgenden Tabelle finden Sie eine allgemeine Übersicht über die Schnellstartkonfiguration der einzelnen Workflows. Die vorkonfigurierten Netzwerk-, Netzwerkdienste- und Profilkonfigurationen können Sie für Schnellstartkonfigurationen verwenden. Ändern Sie für VPN-Konfigurationen das vorhandene VPN-Profil und konfigurieren Sie die VMware SD-WAN Site oder die Non VMware SD-WAN Site. Der letzte Schritt besteht darin, einen neuen Edge zu erstellen und zu aktivieren.

Schritte bei der Schnellstartkonfiguration	SaaS	Non VMware SD-WAN Site-VPN	VMware SD-WAN Site-VPN
Schritt 1: Netzwerk	Internetnetzwerk für Schnellstart auswählen	VPN-Netzwerk für Schnellstart auswählen	VPN-Netzwerk für Schnellstart auswählen
Schritt 2: Netzwerkdienst	Vorkonfigurierte Netzwerkdienste verwenden	Vorkonfigurierte Netzwerkdienste verwenden	Vorkonfigurierte Netzwerkdienste verwenden
Schritt 3: Profil	Internetprofil für Schnellstart auswählen	VPN-Profil für Schnellstart auswählen Cloud-VPN aktivieren und Non VMware SD-WAN Sites konfigurieren	VPN-Profil für Schnellstart auswählen Cloud-VPN aktivieren und VMware SD-WAN Sites konfigurieren
Schritt 4: Edge	Neuen Edge hinzufügen und aktivieren	Neuen Edge hinzufügen und aktivieren	Neuen Edge hinzufügen und aktivieren

Weitere Informationen finden Sie unter Kapitel 20 Schnellstartkonfiguration.

Unterstützte Browser

Für die bestmögliche Erfahrung empfiehlt VMware SD-WAN Google Chrome oder Mozilla Firefox.

Der SD-WAN Orchestrator unterstützt die folgenden Browser.

Qualifizierte Browser	Browserversion
Google Chrome	77 bis 79.0.3945.130
Firefox	69.0.2 bis 72.0.2
Internet Explorer	11.765.17134.0 bis 11.592.18362.0
Microsoft Edge	42.17134.1.0 bis 44.18362.449.0
Safari	12.1.2 bis 13.0.3

Unterstützte Modems

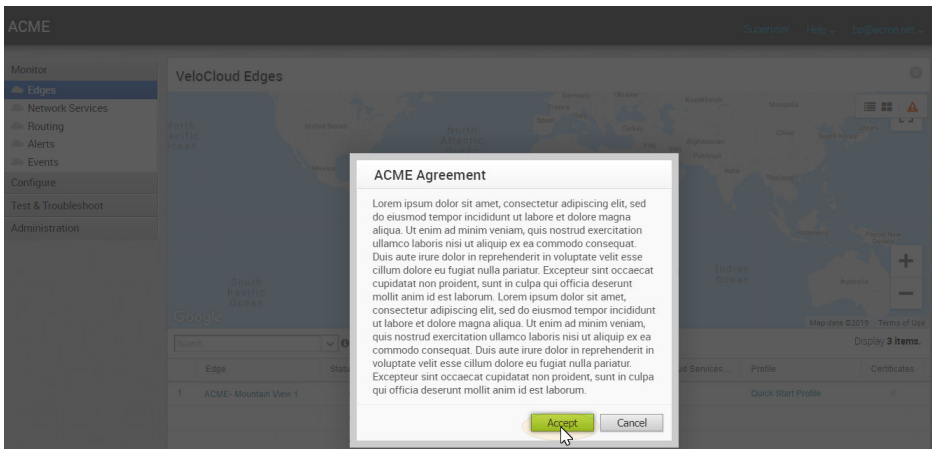
In diesem Abschnitt wird beschrieben, wie Sie eine Liste mit unterstützten Modes erhalten können.

Eine detaillierte Liste unserer unterstützten Modems finden Sie unter http://velocloud.com/get-started/supported-modems

Benutzervereinbarung

4

Einem Enterprise-Superuser oder einem Partner-Superuser wird bei der Anmeldung bei SD-WAN Orchestrator möglicherweise eine Benutzervereinbarung angezeigt. Der Benutzer muss die Vereinbarung akzeptieren, um Zugriff auf SD-WAN Orchestrator zu erhalten. Wenn der Benutzer die Vereinbarung nicht akzeptiert, wird er automatisch abgemeldet.



Anmelden bei VMware SD-WAN Orchestrator mithilfe von SSO für Unternehmensbenutzer

5

Beschreibt, wie Sie sich bei VMware SD-WAN Orchestrator mithilfe von Single Sign-On (SSO) als Unternehmensbenutzer anmelden.

So melden Sie sich bei SD-WAN Orchestrator mithilfe von SSO als Unternehmensbenutzer an:

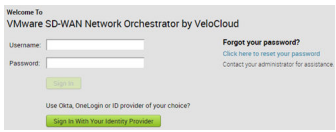
Voraussetzungen

- Stellen Sie sicher, dass Sie die SSO-Authentifizierung in SD-WAN Orchestrator konfiguriert haben. Weitere Informationen finden Sie unter Konfigurieren von Single Sign-On für Unternehmensbenutzer.
- Stellen Sie sicher, dass Sie Rollen, Benutzer und OIDC-Anwendungen für SSO in Ihren bevorzugten Identitätsanbietern eingerichtet haben. Weitere Informationen finden Sie unter Konfigurieren eines IDP für Single Sign-On.

Verfahren

1 Starten Sie als Unternehmensbenutzer in einem Webbrowser eine SD-WAN Orchestrator-Anwendung.

   Der Bildschirm VMware SD-WAN Orchestrator by VeloCloud wird angezeigt.



2 Klicken Sie auf **Beim Identitätsanbieter anmelden (Sign In With Your Identity Provider)**.

3 Geben Sie im Textfeld **Domäne Ihrer Organisation eingeben (Enter your Organization Domain)** den für die SSO-Konfiguration verwendeten Domänennamen ein und klicken Sie auf **Anmelden (Sign In)**.

   Der für SSO konfigurierte Identitätsanbieter authentifiziert den Benutzer und leitet den Benutzer an die konfigurierte SD-WAN Orchestrator-URL weiter.

   Hinweis Sobald sich die Benutzer mithilfe von SSO bei SD-WAN Orchestrator anmelden, können sie sich nicht mehr als native Benutzer anmelden.

Überwachen von Unternehmen

6

Der SD-WAN Orchestrator enthält Überwachungsfunktionen, mit denen Sie verschiedene Leistungs- und Betriebsmerkmale von VMware SD-WAN Edges überwachen können. Auf die Überwachungsfunktionen kann im Bereich **Überwachen (Monitor)** des Navigationsbereichs zugegriffen werden.

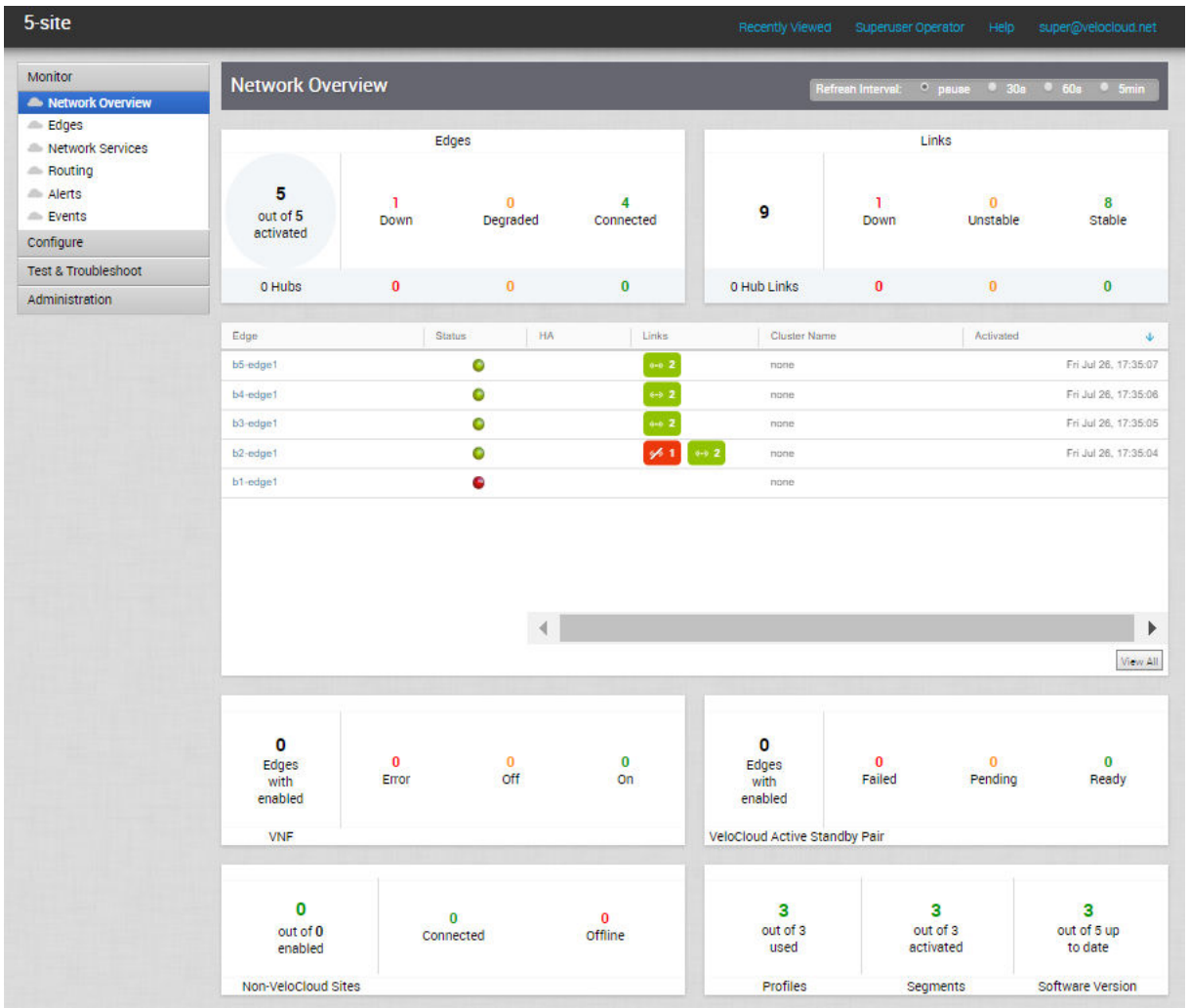
Dieses Kapitel enthält die folgenden Themen:

Navigationsbereich „Überwachen“ (Monitor)

Die folgenden Überwachungsfunktionen werden unter **Überwachen (Monitor)** im Navigationsbereich angezeigt.

Netzwerkübersicht

Die Funktion Netzwerkübersicht (Network Overview) hilft bei der Überwachung von Netzwerken durch Überprüfen der Statusübersicht für den Edge und den Link (aktivierten Edge). Wenn Sie im Navigationsbereich auf **Überwachen (Monitor)** > **Netzwerkübersicht (Network Overview)** klicken, wird der Bildschirm **Netzwerkübersicht (Network Overview)** geöffnet, in dem eine Übersicht über die Unternehmen, in denen SD-WAN Edge-Geräte ausgeführt werden, sowie über Non VMware SD-WAN Sites, Profile, Segmente, Softwareversionen und deren Systemkonfigurationszeit sowie über den Laufzeitstatus bereitgestellt wird.



In der folgenden Tabelle werden die Verbindungsstatustypen und Definitionen für den Edge, Edge-Hub, Link und Hub-Link beschrieben:

Farbe	Bedeutung
Grün	Verbunden
Bernstein	Herabgestuft
Rot	Inaktiv

Im Bildschirm **Netzwerkübersicht (Network Overview)** werden die Zusammenfassungsinformationen zu einem Netzwerk in drei Dashboard-Bereichen angezeigt:

- SD-WAN Edge-Statistik: Enthält die folgenden Informationen zu den Edges und Links:
  - Gesamtzahl der Edges
  - Gesamtanzahl der Edge-Hubs
  - Gesamtzahl der Links
  - Gesamtanzahl der Hub-Links
  - Anzahl der Edges/Edge-Hubs (Verbunden, Herabgestuft und Ausgefallen)
  - Anzahl der Links/Hub-Links (Stabil, Instabil und Ausgefallen)
- Tabelle „Dashboard-Übersicht“: Eine Tabelle, die die zehn wichtigsten Edges, Edge-Hubs, Links oder Hub-Links anzeigt, sortiert nach der letzten Kontaktzeit, basierend auf den ausgewählten Filterkriterien im Abschnitt mit der SD-WAN Edge-Statistik.
- Nicht-Edge-Statistiken: Enthält die folgenden nicht Edge-bezogenen Informationen:
  - Gesamtzahl der VNF-fähigen (Virtual Network Functions) Edges
  - Anzahl der VNF-fähigen Edges (Fehler, Ein und Aus)
  - Gesamtzahl der VMware SD-WAN-Aktiv/Standby-Paar-fähigen Edges
  - Anzahl der VMware SD-WAN-Aktiv/Standby-Paar-fähigen Edges (Fehlgeschlagen, Ausstehend und Bereit)
  - Gesamtzahl der aktivierten Non VMware SD-WAN Sites-Instanzen
  - Anzahl der NVS (Verbunden und Offline)
  - Anzahl der verwendeten Profile von der Gesamtzahl der für das Unternehmen konfigurierten Profile.
  - Anzahl der aktivierten Segmente von der Gesamtzahl der für das Unternehmen konfigurierten Segmente.
  - Anzahl der Edges mit aktueller Softwareversion von der Gesamtzahl der für das Unternehmen konfigurierten Edges.

    Hinweis Die unterstützte Mindestversion des Edge ist 2.4.0. Sie können die Edge-Zielversion, mit der die Edges verglichen werden, mit der Systemeigenschaft `product.edge.version.minimumSupported` ändern.

Sie können außerdem detaillierte Informationen zu einem bestimmten Element im Bildschirm **Netzwerkübersicht (Network Overview)** erhalten, indem Sie auf den Link für das jeweilige Element oder die entsprechende Metrik klicken. Wenn Sie beispielsweise auf den Link **Edge** in der Tabelle „Dashboard-Übersicht“ klicken, gelangen Sie zum Dashboard mit Edge-Details für den ausgewählten Edge.

Sie können das Aktualisierungsintervall für die Informationen, die im Dashboard „Netzwerkübersicht“ (Network Overview) angezeigt werden, auf eine der folgenden Optionen festlegen:

- **Anhalten (pause)**
- **30 Sek. (30s)**
- **60 Sek. (60s)**
- **5 Min. (5min)**

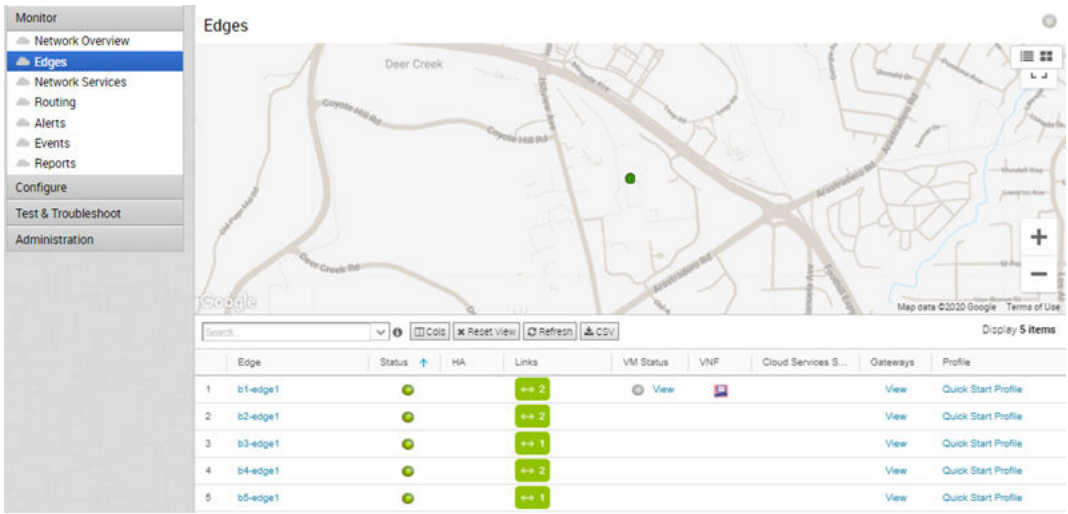
Überwachen von Edges

Sie können den Status der Edges überwachen und die Details jedes Edge anzeigen. Hierzu zählen die WAN-Links, die von den Edges verwendeten Top-Anwendungen, die Nutzungsdaten der Netzwerkquellen und Datenverkehrsziele, die Geschäftspriorität des Netzwerkdatenverkehrs, die Systeminformationen und die Details der mit dem Edge verbundenen Gateways.

So überwachen Sie die Edge-Details:

1 Klicken Sie im Unternehmensportal auf **Überwachen (Monitor) > Edges**.

2 Auf der Seite **Edges** werden die mit dem Unternehmen verbundenen Edges angezeigt.



Auf der Seite werden die folgenden Details der Edges angezeigt:

- Edge-Tabelle – Listet alle im Netzwerk bereitgestellten Edges auf.
- Suche: Geben Sie einen Begriff ein, um nach einem bestimmten Detail zu suchen. Klicken Sie auf den Pfeil nach unten, um die Ansicht anhand bestimmter Kriterien zu filtern.
- Spalte (Column(Cols)): Klicken Sie auf diese Schaltfläche, um die Spalten ein- oder auszublenden. Standardmäßig werden Informationen zum Edge und Status angezeigt.
- Zurücksetzen (Reset): Klicken Sie auf diese Schaltfläche, um die Standardeinstellungen anzuzeigen.

- Aktualisieren (Refresh): Klicken Sie auf diese Schaltfläche, um die angezeigten Details mit den neuesten Daten zu aktualisieren.
- Exportieren (Export): Klicken Sie auf die entsprechende Schaltfläche, um alle Daten in eine Datei im CSV-Format zu exportieren.

Klicken Sie auf den Link zu einem Edge, um die Details im Zusammenhang mit dem ausgewählten Edge anzuzeigen. Klicken Sie auf die entsprechenden Registerkarten, um die jeweiligen Informationen anzuzeigen. Jede Registerkarte enthält oben eine Dropdown-Liste, in der Sie einen bestimmten Zeitraum auswählen können. Die Registerkarte enthält die Details für die ausgewählte Dauer.

Für jeden Edge können Sie die folgenden Details anzeigen:

- Registerkarte „Übersicht“ (Overview)
- Registerkarte „QoE“
- Registerkarte „Transport“
- Registerkarte „Anwendungen (Applications)“
- Registerkarte „Quellen“ (Sources)
- Registerkarte „Ziele (Destinations)“
- Registerkarte „Geschäftspriorität (Business Priority)“
- Registerkarte „System“

Registerkarte „Übersicht“ (Overview)

Auf der Registerkarte „Übersicht (Overview)“ im Überwachungs-Dashboard werden die Details der WAN-Links zusammen mit dem Bandbreitenverbrauch und der Netzwerknutzung angezeigt.

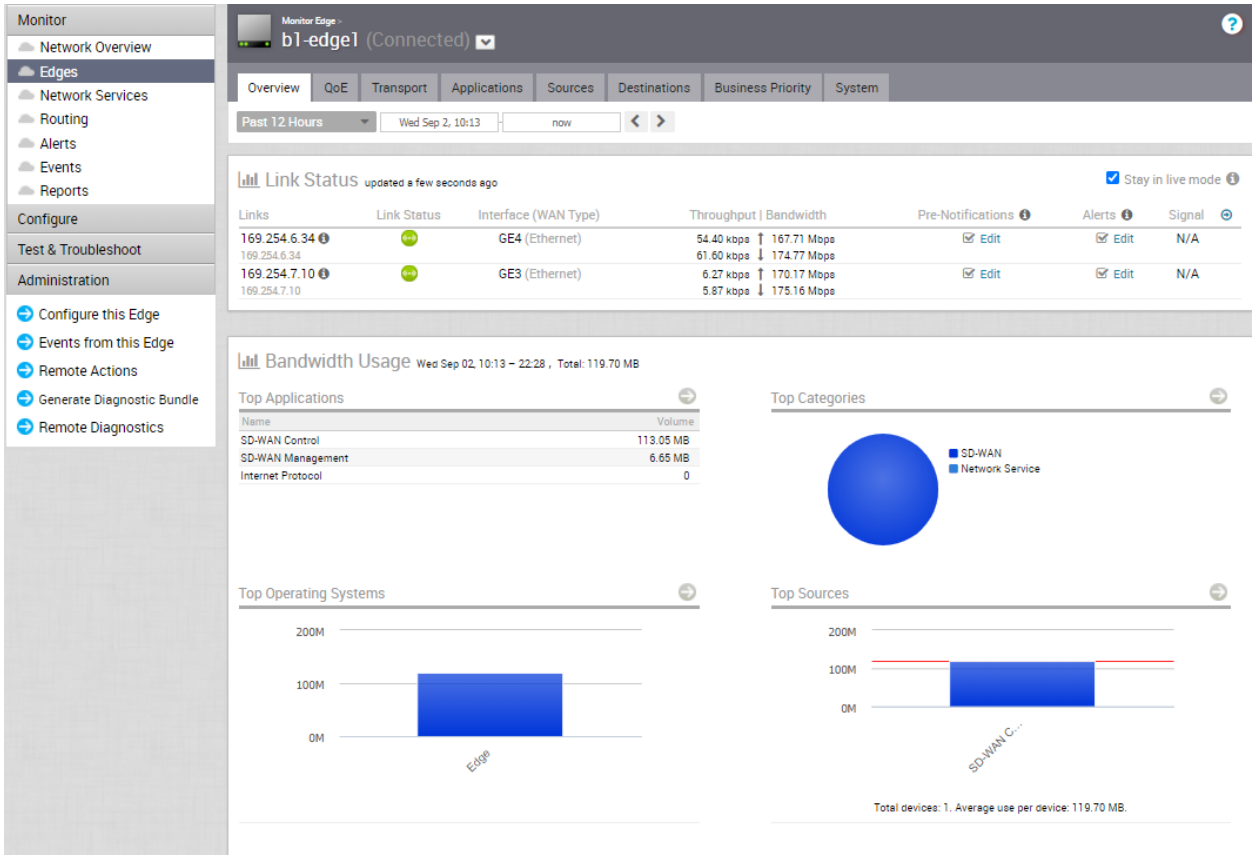
So zeigen Sie die Informationen eines Edge an:

Verfahren

1. Klicken Sie im Unternehmensportal auf **Überwachen (Monitor) > Edges**.
2. Klicken Sie auf den Link zu einem Edge. Die Registerkarte **Übersicht (Overview)** wird standardmäßig angezeigt.

Ergebnisse

Auf der Registerkarte **Übersicht (Overview)** werden die Details der Verbindungen mit Status und der Bandbreitenverbrauch angezeigt.



Sie können die Edge-Informationen live anzeigen, indem Sie das Kontrollkästchen **Im Live-Modus bleiben (Stay in live mode)** aktivieren. Wenn dieser Modus aktiviert ist, wird der Edge live überwacht, und die Daten auf der Seite werden bei jeder Änderung aktualisiert. Der Live-Modus ändert sich nach einem bestimmten Zeitraum automatisch in den Offline-Modus, um die Netzwerklast zu reduzieren.

Im Abschnitt „Verbindungsstatus (Links Status)“ werden die Details der Verbindungen, der Verbindungsstatus, die WAN-Schnittstelle, der Durchsatz, die Bandbreite und das Signal angezeigt.

Der Abschnitt **Hauptverbraucher (Top Consumers)** enthält die grafische Darstellung der Bandbreite und der Netzwerknutzung folgender Elemente: Anwendungen, Kategorien, Betriebssysteme, Quellen und Ziele der Edges. Klicken Sie in jedem Bereich auf **Details anzeigen (View Details)**, um zur entsprechenden Registerkarte zu navigieren und weitere Details anzuzeigen.

Bewegen Sie den Mauszeiger über die Diagramme, um weitere Details anzuzeigen.

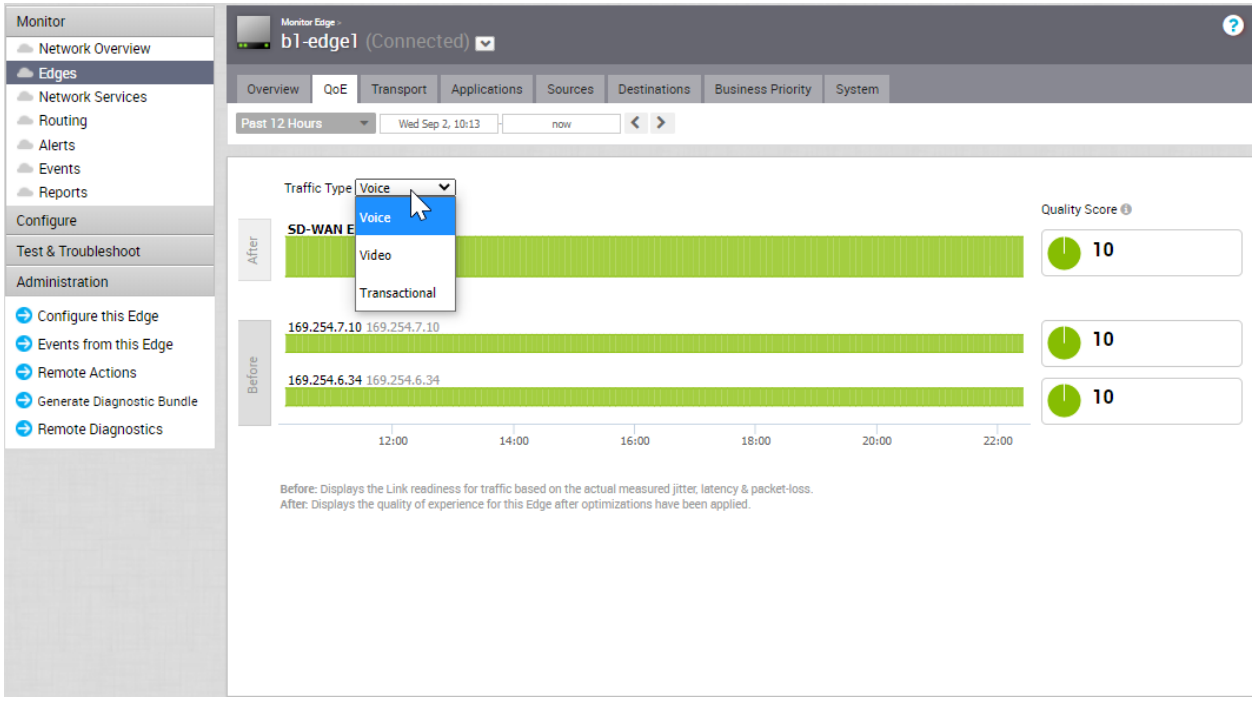
Registerkarte „QoE“

Auf der Registerkarte VMware SD-WAN **Quality of Experience (QoE)** wird der VeloCloud Quality Score (VQS) für verschiedene Anwendungen angezeigt. Der VQS bewertet die Erfahrungsqualität (Quality of Experience) einer Anwendung, die ein Netzwerk für einen bestimmten Zeitraum liefern kann.

Klicken Sie auf die Registerkarte **Überwachen (Monitor) > Edges > QoE**, um die folgenden Details anzuzeigen.

Datenverkehrstyp

Es gibt drei verschiedene Datenverkehrstypen, die Sie auf der Registerkarte **QoE** überwachen können (Sprache, Video und Transaktional). Sie können den Mauszeiger über eine WAN-Netzwerkverbindung oder die aggregierte Verbindung bewegen, um eine Übersicht über Latenz, Jitter und Paketverlust anzuzeigen.



VeloCloud Quality Score

Der VeloCloud Quality Score (VQS) bewertet die Erfahrungsqualität (Quality of Experience) einer Anwendung, die ein Netzwerk für einen bestimmten Zeitraum liefern kann. Einige Beispiele für Anwendungen sind: Video-, Sprach- und Transaktionsanwendungen. Die Optionen für die Bewertung von QoE werden in der folgenden Tabelle angezeigt.

Bewertungsfarbe	Bewertungsoption	Definition
Grün	Gut (Good)	Alle Metriken sind besser als die objektiven Schwellenwerte. Anwendungs-SLA erfüllt/übertroffen.
Gelb	Mittel (Fair)	Einige oder alle Metriken liegen zwischen dem Zielwert und dem Maximalwert. Anwendungs-SLA ist teilweise erfüllt.
Rot	Schlecht (Poor)	Einige oder alle Metriken haben den Maximalwert erreicht oder überschritten. Anwendungs-SLA ist nicht erfüllt.

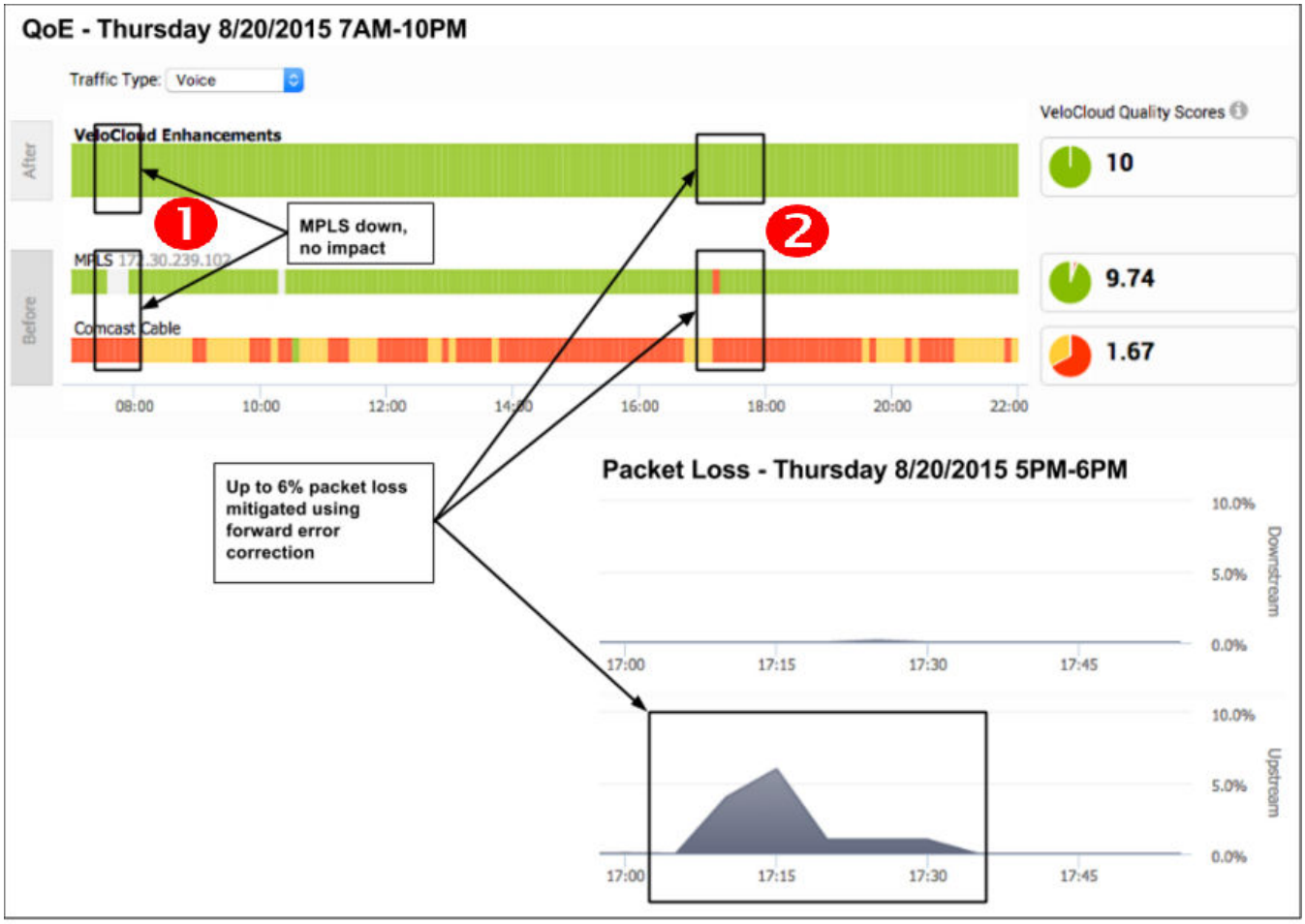
Beispiel für QoE

Die folgenden Abbildungen zeigen Beispiele für QoE mit Problemen im Zusammenhang mit Vorher/Nachher-Sprachdatenverkehrsszenarien und wie VMware SD-WAN diese behoben hat. Bei den roten Zahlen in den folgenden Abbildungen handelt es sich um die Szenarionummern in der Tabelle.

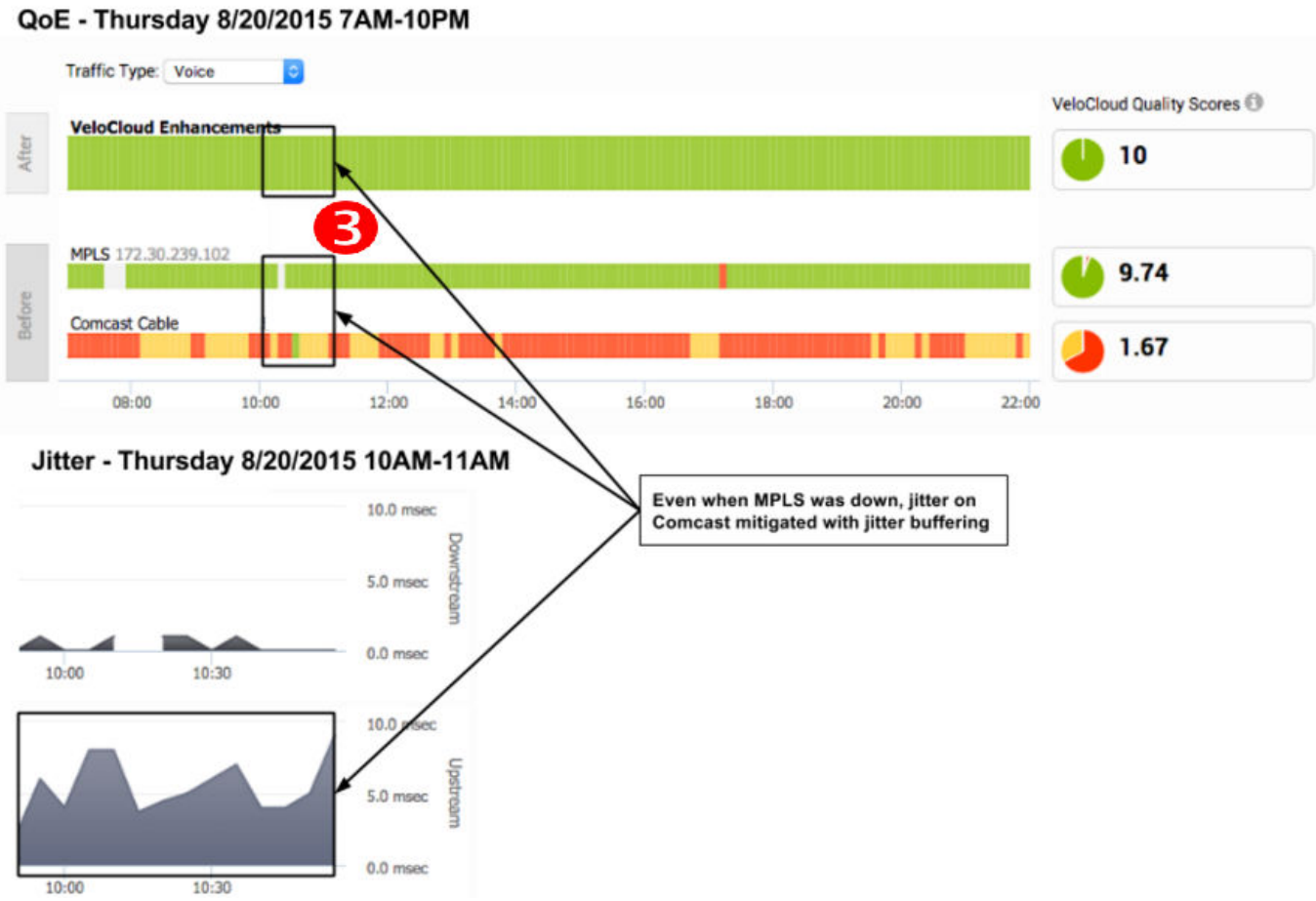
Tabelle mit QoE-Beispiel

Szenario	Problem	VMware SD-WAN-Lösung
1	MPLS ist ausgefallen	Link-Steuerung
2	Paketverlust	Vorwärtsgerichtete Fehlerkorrektur
3	MPLS ist ausgefallen; Jitter bei Comcast	Link-Steuerung und Link-Pufferung

Szenario 1 und 2: Link-Steuerung und vorwärtsgerichtete Fehlerkorrektur – Lösungsbeispiel



Szenario 3: Link-Steuerung und Jitter-Pufferung – Lösungsbeispiel



Registerkarte „Transport“

Sie können die mit einem bestimmten Edge verbundenen WAN-Links zusammen mit dem Status, den Schnittstellendetails und andere Metriken überwachen.

Auf der Registerkarte **Überwachen (Monitor) > Edges > Transport** können Sie jederzeit einsehen, welcher Link oder welche Transportgruppe für den Datenverkehr verwendet wird und wie viele Daten gesendet werden.

Wenn Sie auf die Registerkarte **Transport** klicken, wird der Bildschirm **Verbindungen (Links)** standardmäßig angezeigt. In diesem Bildschirm werden die gesendeten und empfangenen Daten für Ihre Verbindungen angezeigt. Die mit einem Edge verknüpften Verbindungen werden unten im Bildschirm unter der Spalte „Verbindung (Link)“ zusammen mit dem Status für Cloud und VPN, WAN-Schnittstelle, Anwendungsdetails und Details zu Bytes angezeigt.

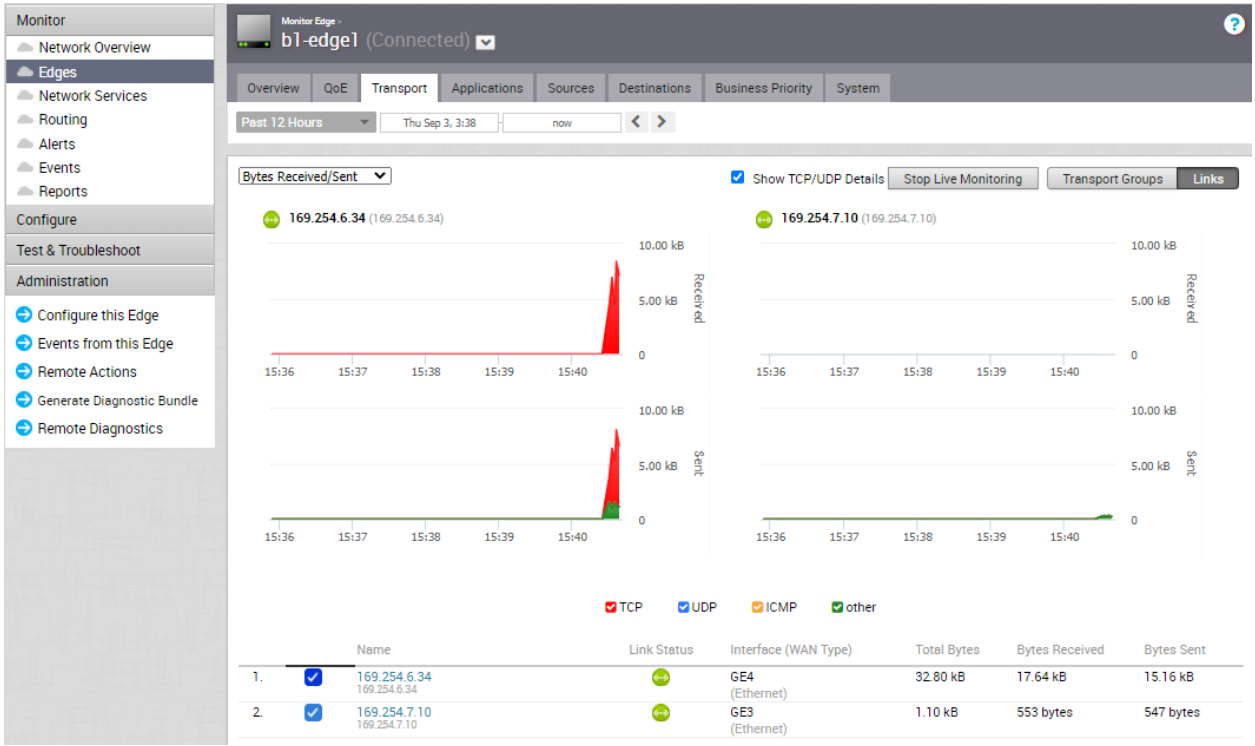
Bewegen Sie den Mauszeiger über die Diagramme, um weitere Details anzuzeigen.

Oben auf der Seite können Sie einen bestimmten Zeitraum auswählen, um die Details der Links anzuzeigen, die für die gewählte Dauer verwendet wurden.

Klicken Sie auf **Transportgruppen (Transport Groups)**, um die Verbindungen anzuzeigen, die in eine der folgenden Kategorien gruppiert sind: Öffentlich verkabelt (Public Wired), Öffentlich drahtlos (Public Wireless) oder Privat verkabelt (Private Wired).

Sie können auswählen, ob die Informationen live angezeigt werden sollen, indem Sie auf die Option **Live-Überwachung starten (Start Live Monitoring)** klicken. Wenn dieser Modus aktiviert ist, können Sie die Live-Überwachung der Links und der Transportgruppen anzeigen. Die Live-Überwachung ist nützlich, um aktive Tests durchzuführen und den durchschnittlichen Durchsatz zu berechnen. Sie ist auch für die Fehlerbehebung bei der Sicherheitskonformität und für die Überwachung der Nutzung von Datenverkehrsrichtlinien in Echtzeit vorteilhaft.

Aktivieren Sie im Bildschirm **Live-Überwachung (Live Monitoring)** das Kontrollkästchen **TCP/UDP-Details anzeigen (Show TCP/UDP Details)**, um Details zur Verbindungsnutzung auf Protokollebene anzuzeigen.

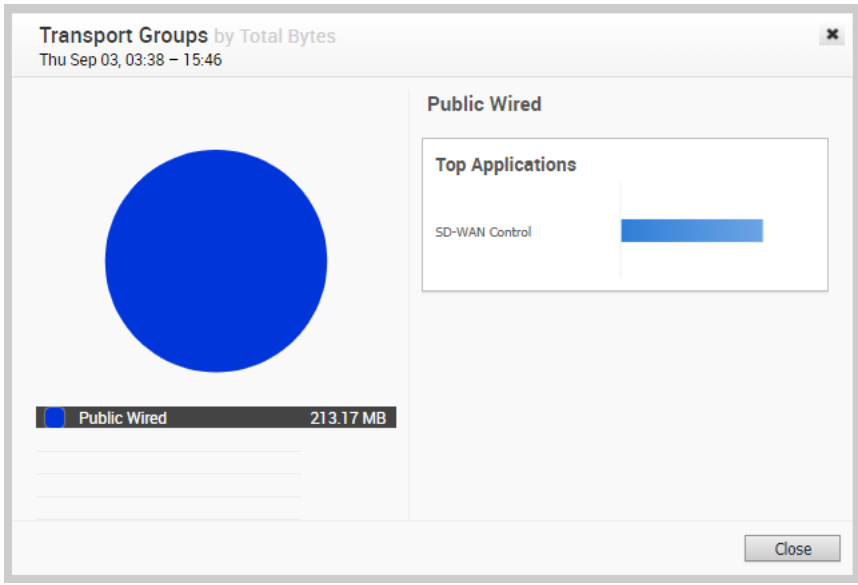


Standardmäßig ist das Kontrollkästchen **Y-Achse gleichmäßig skalieren (Scale Y-axis evenly)** aktiviert. Mit dieser Option wird die Y-Achse zwischen den Diagrammen synchronisiert. Falls erforderlich, können Sie diese Option deaktivieren.

Wählen Sie die Metriken im Dropdown-Menü aus, um die Details im Zusammenhang mit dem ausgewählten Parameter anzuzeigen. Im unteren Bereich werden die Details der ausgewählten Metriken für die Links oder die Transportgruppen angezeigt.

Klicken Sie auf den Pfeil vor dem Link-Namen oder der Transportgruppe, um die aufgeschlüsselten Details anzuzeigen. Klicken Sie auf die Links, die in der Spalte mit den Metriken angezeigt werden, um Drilldown-Berichte mit weiteren Details anzuzeigen.

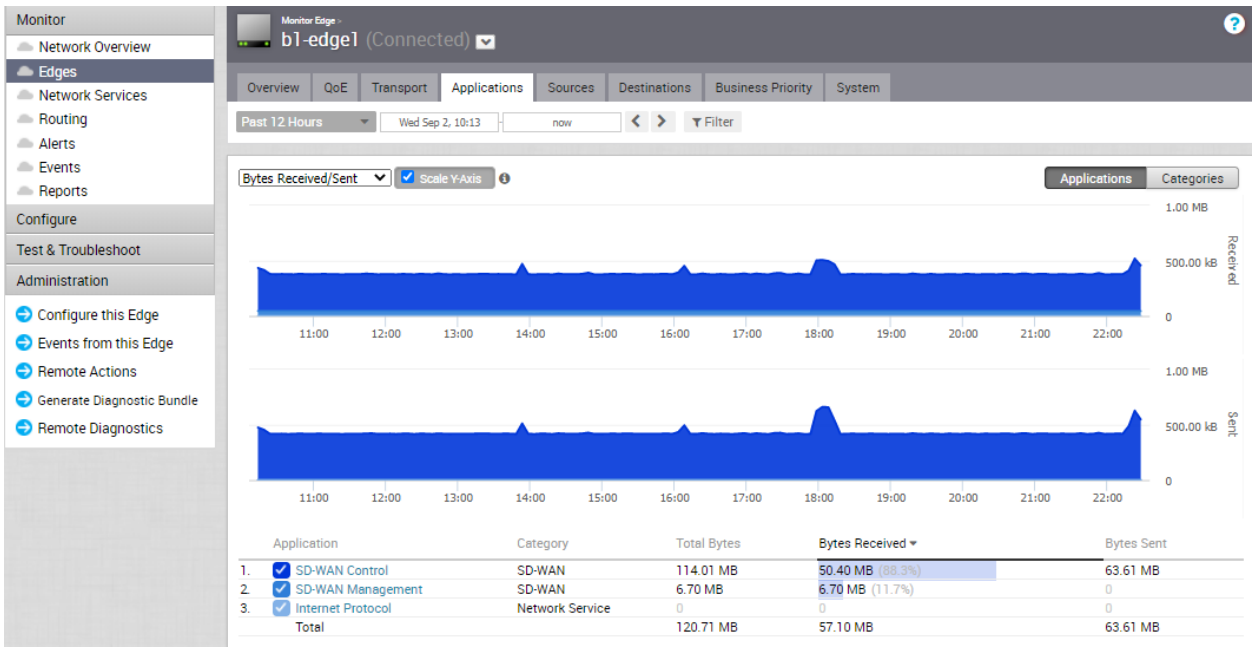
Die folgende Abbildung zeigt einen detaillierten Bericht der Transportgruppen mit Top-Anwendungen.



Registerkarte „Anwendungen (Applications)“

Sie können die Netzwerknutzung von Anwendungen oder Anwendungskategorien, die von einem bestimmten Edge verwendet werden, überwachen.

Klicken Sie auf die Registerkarte **Überwachen (Monitor) > Edges > Anwendungen (Applications)**, um Folgendes anzuzeigen:



Oben auf der Seite können Sie einen bestimmten Zeitraum auswählen, um die Details der Anwendungen anzuzeigen, die für die gewählte Dauer verwendet wurden.

Klicken Sie auf **Kategorien (Categories)**, um ähnliche Anwendungen anzuzeigen, die in Kategorien gruppiert sind.

Bewegen Sie den Mauszeiger über die Diagramme, um weitere Details anzuzeigen.

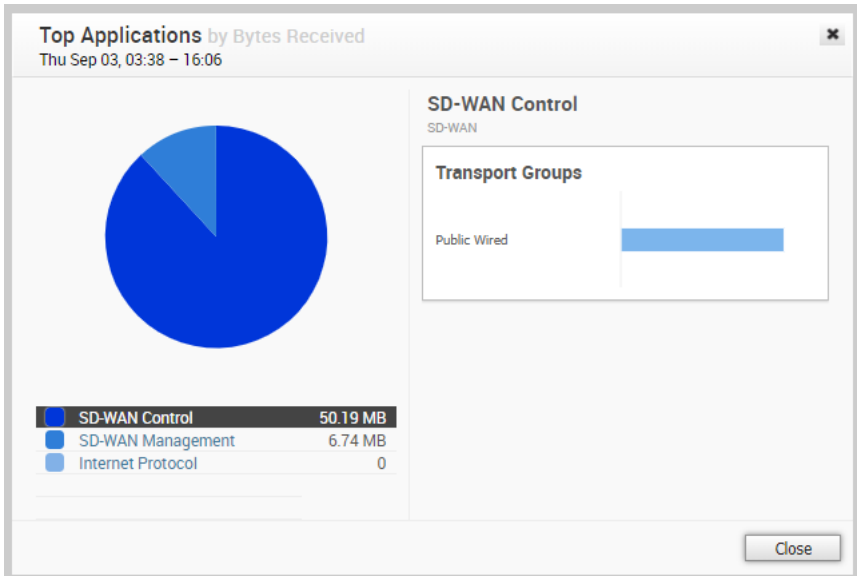
Wählen Sie die Metriken im Dropdown-Menü aus, um die Details im Zusammenhang mit dem ausgewählten Parameter anzuzeigen.

Standardmäßig ist das Kontrollkästchen **Y-Achse gleichmäßig skalieren (Scale Y-axis evenly)** aktiviert. Mit dieser Option wird die Y-Achse zwischen den Diagrammen synchronisiert. Falls erforderlich, können Sie diese Option deaktivieren.

Im unteren Bereich werden die Details der ausgewählten Metriken für die Anwendungen oder Kategorien angezeigt.

Klicken Sie auf die Links, die in der Spalte mit den Metriken angezeigt werden, um Drilldown-Berichte mit weiteren Details anzuzeigen.

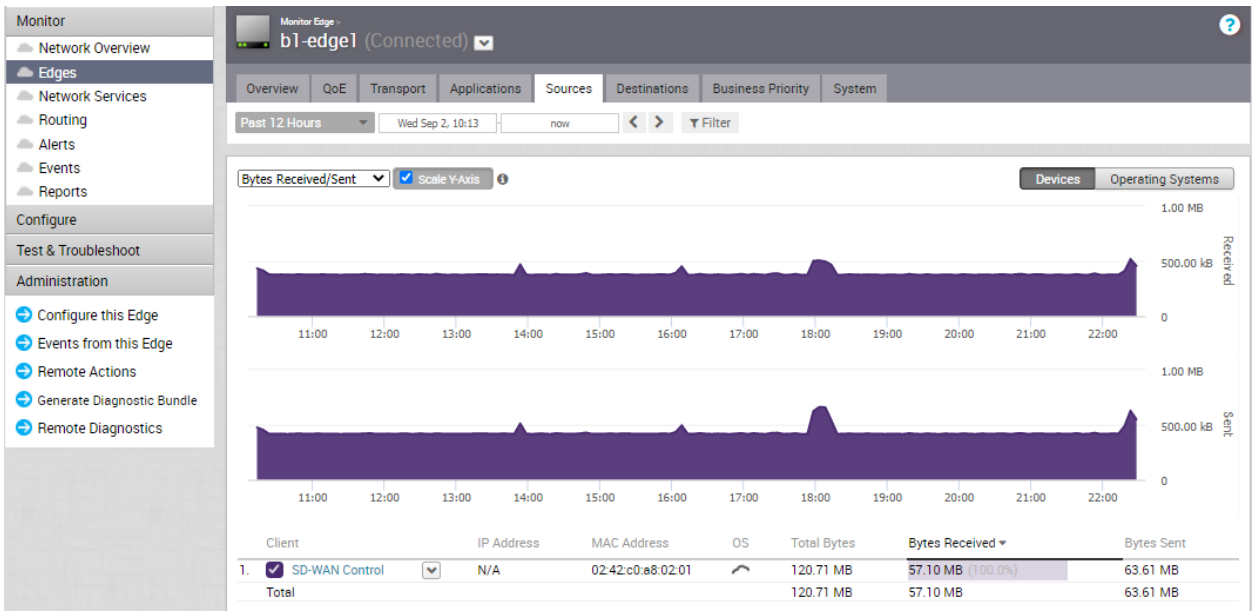
Die folgende Abbildung zeigt einen detaillierten Bericht zu den wichtigsten Anwendungen.



Registerkarte „Quellen“ (Sources)

Sie können die Netzwerknutzung von Geräten und Betriebssystemen für einen bestimmten Edge überwachen.

Klicken Sie auf **Überwachen (Monitor) > Edges > Quellen (Sources)**, um Folgendes anzuzeigen:



Oben auf der Seite können Sie einen bestimmten Zeitraum auswählen, um die Details der Clients anzuzeigen, die für die gewählte Dauer verwendet wurden.

Klicken Sie auf **Betriebssysteme (Operating Systems)**, um den Bericht auf der Grundlage der in den Geräten verwendeten Betriebssysteme anzuzeigen.

Wählen Sie die Metriken im Dropdown-Menü aus, um die Details im Zusammenhang mit dem ausgewählten Parameter anzuzeigen.

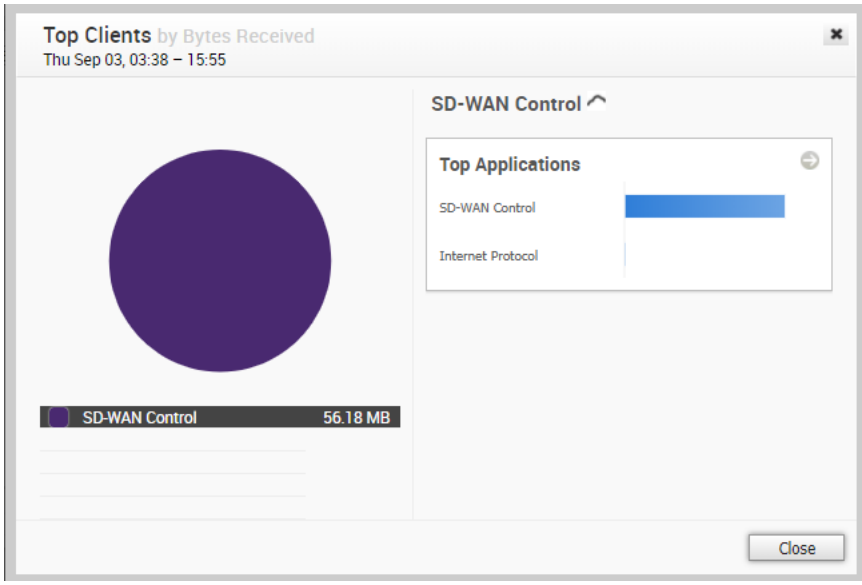
Standardmäßig ist das Kontrollkästchen **Y-Achse gleichmäßig skalieren (Scale Y-axis evenly)** aktiviert. Mit dieser Option wird die Y-Achse zwischen den Diagrammen synchronisiert. Falls erforderlich, können Sie diese Option deaktivieren.

Bewegen Sie den Mauszeiger über die Diagramme, um weitere Details anzuzeigen.

Im unteren Bereich werden die Details der ausgewählten Metriken für die Geräte oder Betriebssysteme angezeigt.

Klicken Sie auf die Links, die in der Spalte mit den Metriken angezeigt werden, um Drilldown-Berichte mit weiteren Details anzuzeigen.

Die folgende Abbildung zeigt einen detaillierten Bericht zu den wichtigsten Clients.

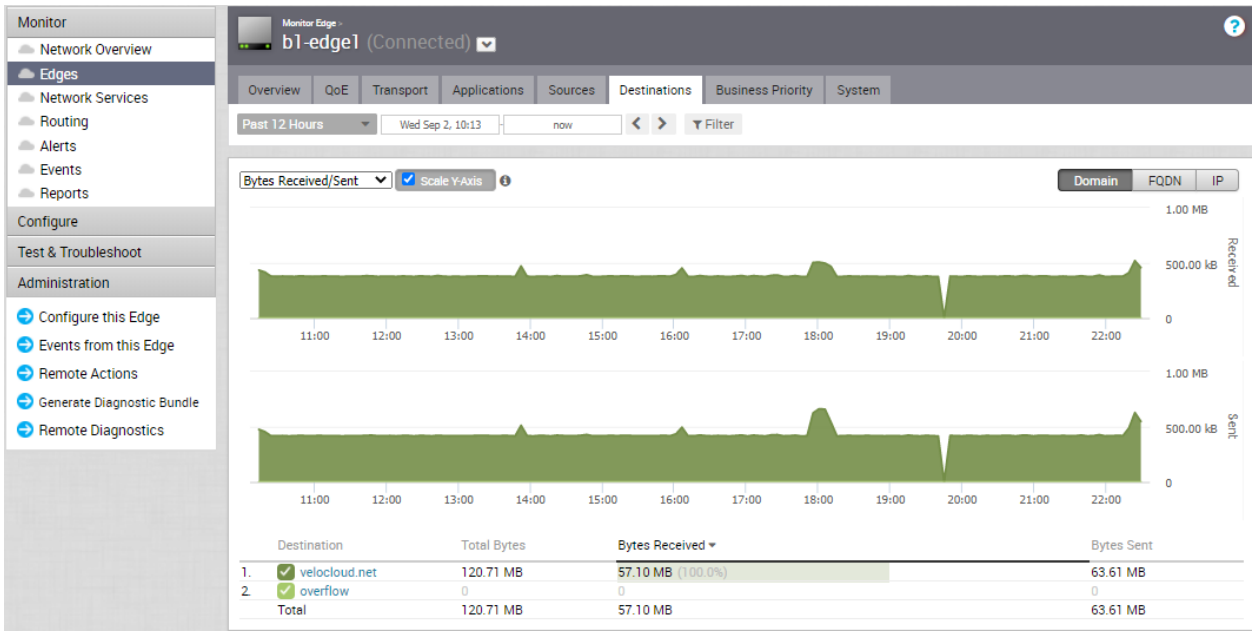


Klicken Sie auf die Pfeile neben **Top-Anwendungen (Top Applications)**, um zur Registerkarte **Anwendungen (Applications)** zu navigieren.

Registerkarte „Ziele (Destinations)“

Sie können die Netzwerknutzungsdaten der Ziele des Netzwerkdatenverkehrs überwachen.

Klicken Sie auf die Registerkarte **Überwachen (Monitor) > Edges > Ziele (Destinations)**, um Folgendes anzuzeigen:



Oben auf der Seite können Sie einen bestimmten Zeitraum auswählen, um die Details der Ziele anzuzeigen, die für die gewählte Dauer verwendet wurden.

Sie können den Bericht zu den Zielen nach **Domäne (Domain)**, **FQDN** oder **IP**-Adresse anzeigen. Klicken Sie auf den relevanten Typ, um die entsprechenden Informationen anzuzeigen.

Bewegen Sie den Mauszeiger über die Diagramme, um weitere Details anzuzeigen.

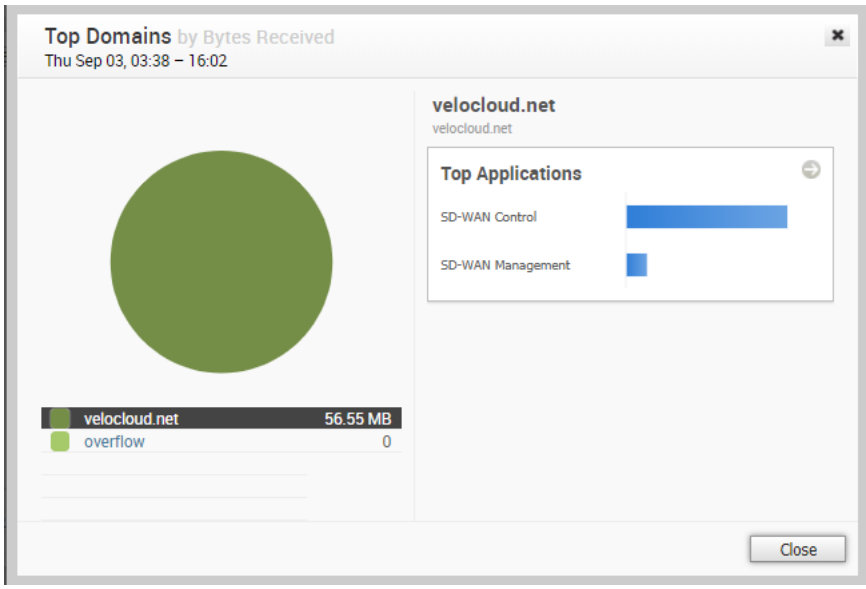
Wählen Sie die Metriken im Dropdown-Menü aus, um die Details im Zusammenhang mit dem ausgewählten Parameter anzuzeigen.

Standardmäßig ist das Kontrollkästchen **Y-Achse gleichmäßig skalieren (Scale Y-axis evenly)** aktiviert. Mit dieser Option wird die Y-Achse zwischen den Diagrammen synchronisiert. Falls erforderlich, können Sie diese Option deaktivieren.

Im unteren Bereich werden die Details der ausgewählten Metriken für die Ziele nach gewähltem Typ angezeigt.

Klicken Sie auf die Links, die in der Spalte mit den Metriken angezeigt werden, um Drilldown-Berichte mit weiteren Details anzuzeigen.

Die folgende Abbildung zeigt einen detaillierten Bericht zu den wichtigsten Domänen.

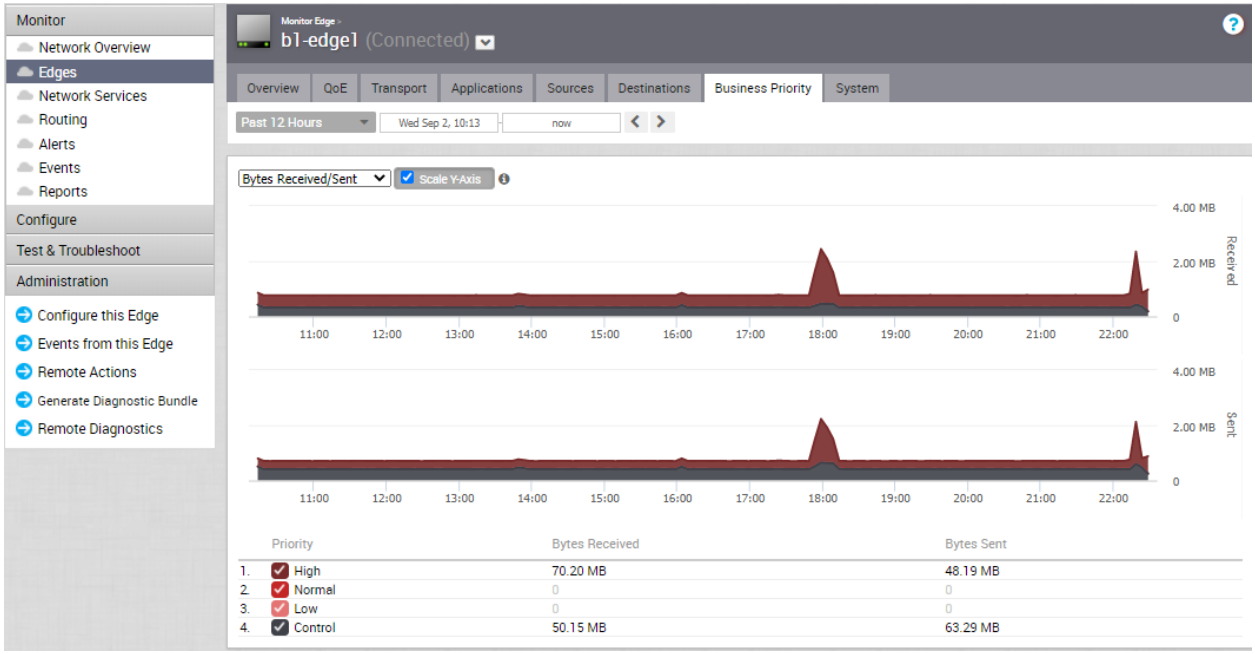


Klicken Sie auf die Pfeile neben **Top-Anwendungen (Top Applications)**, um zur Registerkarte **Anwendungen (Applications)** zu navigieren.

Registerkarte „Geschäftspriorität (Business Priority)“

Sie können die Merkmale der Unternehmensrichtlinie entsprechend der Priorität und den zugehörigen Netzwerknutzungsdaten für einen bestimmten Edge überwachen.

Klicken Sie auf **Überwachen (Monitor) > Edges > Geschäftspriorität (Business Priority)**, um Folgendes anzuzeigen:



Oben auf der Seite können Sie einen bestimmten Zeitraum auswählen, um die Details der Prioritäten für die ausgewählte Dauer anzuzeigen.

Wählen Sie die Metriken im Dropdown-Menü aus, um die Details im Zusammenhang mit dem ausgewählten Parameter anzuzeigen.

Standardmäßig ist das Kontrollkästchen **Y-Achse gleichmäßig skalieren (Scale Y-axis evenly)** aktiviert. Mit dieser Option wird die Y-Achse zwischen den Diagrammen synchronisiert. Falls erforderlich, können Sie diese Option deaktivieren.

Bewegen Sie den Mauszeiger über die Diagramme, um weitere Details anzuzeigen.

Im unteren Bereich werden die Details der ausgewählten Metriken für die Geschäftsprioritäten angezeigt.

Registerkarte „System“

Sie können die detaillierte Netzwerknutzung durch das System für einen bestimmten Edge anzeigen.

So zeigen Sie die Details der Systeminformationen an:

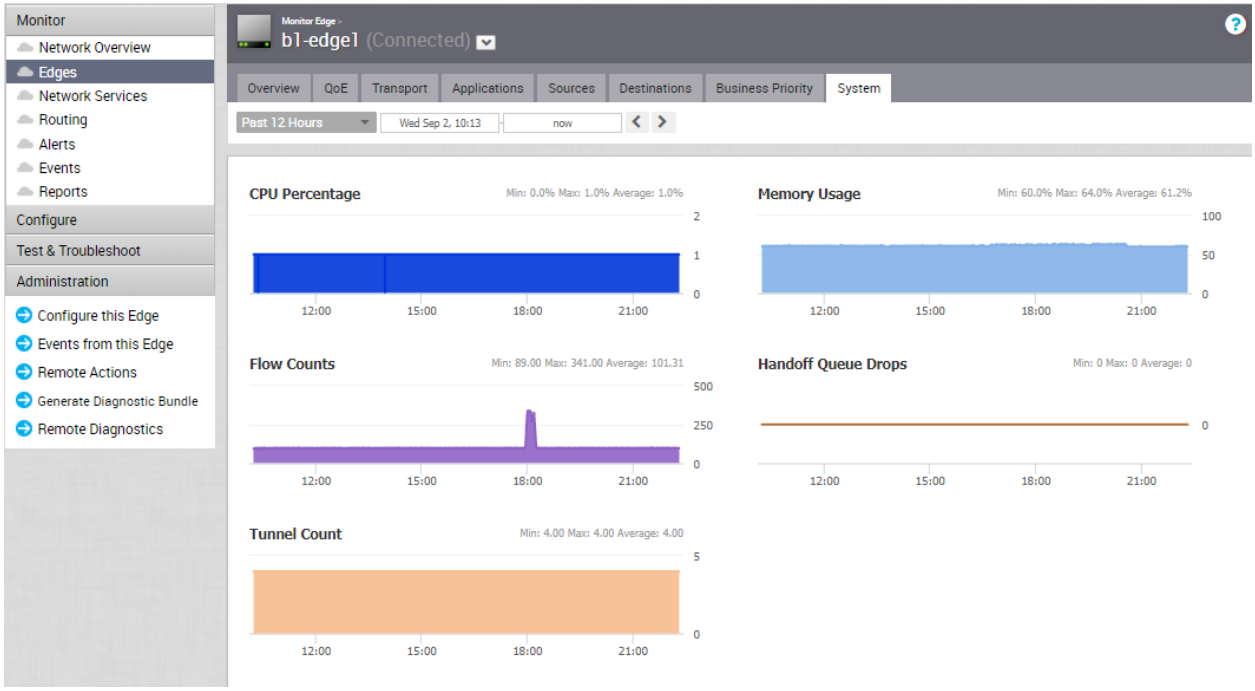
Verfahren

1 Klicken Sie im Unternehmensportal auf **Überwachen (Monitor) > Edges**.

2 Klicken Sie auf den Link zu einem Edge und dann auf die Registerkarte **System**.

Ergebnisse

Auf der Registerkarte **System** werden die Details der Netzwerknutzung durch das System für den ausgewählten Edge angezeigt.



Die Seite enthält eine grafische Darstellung der Nutzungsdaten der folgenden Elemente über den ausgewählten Zeitraum zusammen mit den Mindest-, Höchst- und Durchschnittswerten.

- **CPU-Prozentsatz (CPU Percentage)**: Der Prozentsatz der CPU-Nutzung.
- **Arbeitsspeichernutzung (Memory Usage)**: Prozentsatz der Arbeitsspeichernutzung.
- **Flow-Anzahl (Flow Counts)**: Die Anzahl der Datenverkehrsströme.
- **Verworfene Pakete der Übergabewarteschlange (Handoff Queue Drops)**: Anzahl der Pakete, die aufgrund der in die Warteschlange gestellten Übergabe verworfen werden.
- **Tunnelanzahl (Tunnel Count)**: Anzahl der Tunnelsitzungen.

Bewegen Sie den Mauszeiger über die Diagramme, um weitere Details anzuzeigen.

Rollups und Aufbewahrung von Flow-Statistiken

In Version 3.3.0 speichert der SD-WAN Orchestrator nur Flow-Statistiken mit hoher Auflösung, um die Darstellung zu verbessern und Fehlerbehebungsfunktionen bereitzustellen. Ab Version 3.3.2 unterstützt SD-WAN Orchestrator die Aufbewahrung von Flow-Statistiken für bis zu einem Jahr, indem für die Flow-Statistiken aller Edges täglich ein Rollup durchgeführt wird. Aktuell werden Rollups der täglichen Flow-Statistiken nur für lokale Kunden unterstützt.

Aggregieren der Flow-Statistiken

Der SD-WAN Orchestrator aggregiert derzeit Flow-Statistiken aus einer höheren Auflösung (alle 5 Minuten) in ein lesbares Format mit geringerer Auflösung (alle 24 Stunden). In den folgenden Tabellen werden Informationen zur Unterstützung des Rollups und der Aufbewahrung von Flow-Statistiken zusammengefasst.

Tabelle 6-1. Rollup der Flow-Statistiken – Unterstützung

Auflösung	Rollup vor 3.3.0	Rollup nach 3.3.0	Rollup nach 3.3.2
Hoch	5 Minuten	5 Minuten	5 Minuten
Mittel	2 Stunden	Veraltet	Nicht unterstützt
Niedrig	8 Stunden	Veraltet	24 Stunden

Tabelle 6-2. Aufbewahrung der Flow-Statistiken – Unterstützung

Auflösung	Aufbewahrung vor 3.3.0	Aufbewahrung nach 3.3.0 für lokal	Aufbewahrung von 3.3.0 für gehostet	Aufbewahrung nach 3.3.2 für lokal	Aufbewahrung von 3.3.2 für gehostet
Hoch	6-10 Wochen	14 Tage (Standardwert), 31 Tage (Höchstwert)	14 Tage	14 Tage	14 Tage
Mittel	10-14 Wochen	Veraltet	Veraltet	Veraltet	Veraltet
Niedrig	Bis zu 1 Jahr	Veraltet	Veraltet	Bis zu 1 Jahr	Veraltet

Häufig gestellte Fragen

- Wie können tägliche Rollups für Flow-Statistiken nach einem 3.3.2-Upgrade aktiviert werden?

  Zum Aktivieren täglicher Rollups für Flow-Statistiken setzen Sie die Systemeigenschaft `flowStats.daily.rollup.enabled` auf `true`.

- Wie hoch ist die maximale Anzahl an Flows, für die täglich ein Rollup pro Edge durchgeführt wird?

  Standardmäßig wird täglich ein Rollup für maximal eine Million Flows pro Edge durchgeführt. Durchschnittlich werden somit alle 5 Minuten 3500 Flows verarbeitet. Sie können die Anzahl der Flows, für die täglich ein Rollup pro Edge durchgeführt wird, mithilfe der Systemeigenschaft `flowStats.daily.rollup.flowLimit` ändern.

- Wird für Hub-Flows ein Rollup durchgeführt?

  Standardmäßig ist das Durchführen von Rollups für Hub-Flows deaktiviert. Sie können Hub-Flows mithilfe der Systemeigenschaft `flowStats.daily.rollup.edgeflowLimit` aktivieren, die das Schlüsselwertpaar `<edgeId>:<numFlows>` enthält. Hub-Flows mit hoher Auflösung können maximal 15 Tage angezeigt werden.

- Kann die Aufbewahrungsrichtlinie von Flow-Statistiken konfiguriert werden?

  Die Aufbewahrungsrichtlinie für zusammengefasste Statistiken kann im SD-WAN Orchestrator mithilfe der Systemeigenschaft `retentionWeeks.flowStats.daily` konfiguriert werden. Für die Aufbewahrung der zusammengefassten Flow-Statistiken kann ein beliebiger Zeitraum zwischen 1 und 52 Wochen konfiguriert werden.

- Können Flow-Statistiken nach der Aktivierung von Rollups länger als 15 Tage über die Benutzeroberfläche abgefragt werden?

Nein. Das Durchführen von Rollups für Flow-Statistiken zur längeren Aufbewahrung wird von der tatsächlichen Möglichkeit zur Abfrage dieser Flow-Statistiken getrennt. Sie können die Anzahl der Tage festlegen, die die Flows mithilfe der Systemeigenschaft `session.options.maxFlowstatsRetentionDays` abgefragt werden sollen.

- Sind nach dem Aktivieren dieser Funktion datenseitig negative Auswirkungen zu erwarten?

  Obwohl bei aggregierten Ergebnissen keine negativen Auswirkungen beobachtet werden, weisen die Zeitreihendiagramme auf der SD-WAN Orchestrator-Benutzeroberfläche aufgrund der Anzeige zusammengefasster Reihenstatistiken einen Genauigkeitsverlust auf.

- Welche negativen Auswirkungen sind bezüglich der Systemlast zu verzeichnen?

  Da beim Rollup für tägliche Flow-Statistiken Ergebnisse anhand der vollauflösenden Tabelle aggregiert und separat gespeichert werden, kommt es aufgrund der zusätzlichen Verarbeitungsprozesse, die von MySQL zum Aggregieren der Ergebnisse benötigt werden, zu einer zwangsläufigen Steigerung der Systemlast (CPU/durchschnittliche Last).

- Mit welchen Auswirkungen ist beim Speichern lokaler Bereitstellungen zu rechnen?

  Da beim Rollup für tägliche Flow-Statistiken Ergebnisse anhand der hochauflösenden Tabelle aggregiert und separat gespeichert werden, geht VMware SD-WAN davon aus, dass die lokalen Kunden ihren Speicherbedarf zur Aufnahme zusammengefasster Statistiken planen müssen. Durchschnittlich verbrauchen zusammengefasste Flows 1/8 des für hochauflösende Statistiken notwendigen Speicherplatzes. Dieser Wert hängt jedoch stark von der Beschaffenheit der täglichen Flows ab, die vom Edge gesendet werden. In diesem Fall liegt der Anstieg des Speicherverbrauchs zusammengefasster Statistiken deutlich unter dem der hochauflösenden Statistiken. Für Kunden, die mit einem kleineren Datenträger beginnen, empfiehlt VMware SD-WAN die Verwendung logischer Volumes, damit die Speicherkapazität bei einer Zunahme der Edges erhöht werden kann.

Ändern des Aufbewahrungszeitraums

Für die Aufbewahrung hochauflösender Flow-Statistiken kann ein beliebiger Zeitraum zwischen 1 und 31 Tagen konfiguriert werden. Ab Version 3.3.0 wurde die Konfigurationsgranularität zur Aufbewahrung hochauflösender Flow-Statistiken von Monaten in Tage geändert. Operatoren können den Aufbewahrungszeitraum ändern, indem sie eine Systemeigenschaft erstellen. Führen Sie die folgenden Schritte aus, um eine Systemeigenschaft zum Ändern des Aufbewahrungszeitraums zu erstellen.

1 Klicken Sie im Navigationsbereich von SD-WAN Orchestrator auf **Systemeigenschaften (System Properties)**.

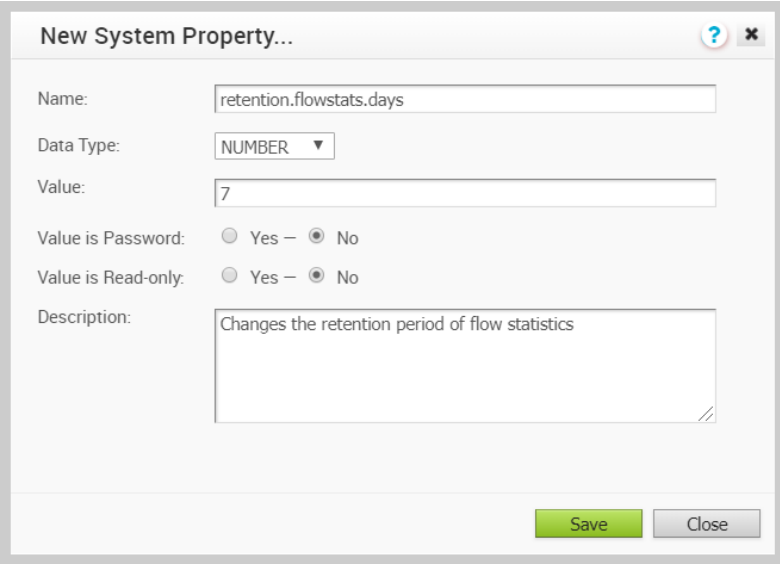
2 Klicken Sie auf der Seite **Systemeigenschaften (System Properties)** auf die Schaltfläche **Neue Systemeigenschaften (New System Properties)**.

3 Gehen Sie im Dialogfeld **Neue Systemeigenschaft (New System Property)** folgendermaßen vor:

   a Geben Sie im Textfeld **Name** den Wert `retention.flowstats.days` ein.

b Wählen Sie im Dropdown-Menü **Datentyp (Data Type)** die Option **Zahl (Number)** aus.

c Geben Sie im Textfeld **Wert (Value)** den Aufbewahrungszeitraum in Tagen ein.



4 Klicken Sie auf **Speichern (Save)**.

Überwachen von Netzwerkdiensten

Netzwerkdienste sind unter der Option **Überwachen (Monitor)** im Navigationsbereich verfügbar. Dort wird der Status der VPN-Tunnel für Non VMware SD-WAN Sites angezeigt.

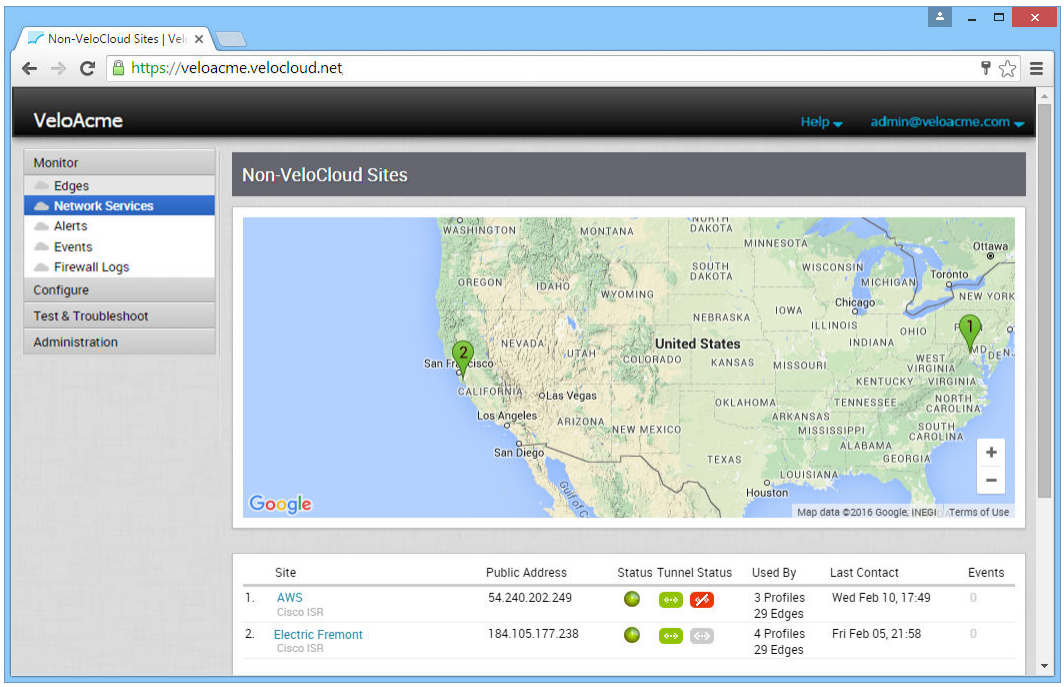
Sie können in der Spalte **Site** auf eine Non VMware SD-WAN Site klicken, um ein Dialogfeld zu öffnen, in dem Sie Informationen zu Ihrer Site ändern können.

Zu den Non VMware SD-WAN Sites-Typen gehören:

- IaaS: AWS
- CWS: Zscaler
- Non VMware SD-WAN Site: Palo Alto, Sonic Wall
- Nicht-VMware SD-WAN Hub

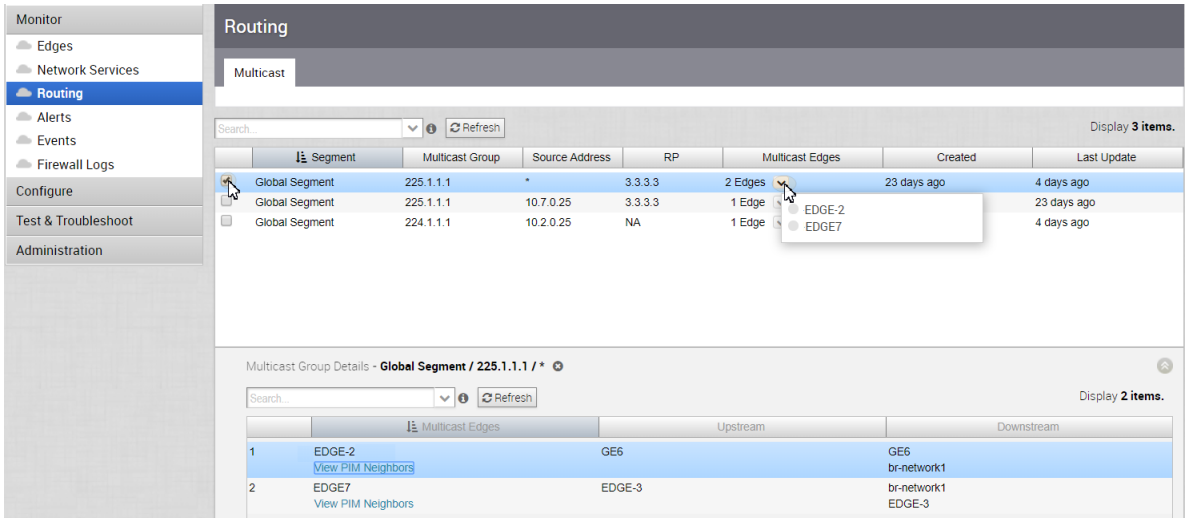
Im Non VMware SD-WAN Site-Bildschirm werden der Status und der Tunnelstatus angezeigt. Die Arten der Statusergebnisse sind unten aufgelistet:

Farbe	Bedeutung
Grün	Verbunden
Rot	Offline/Getrennt
Grau	Nicht aktiviert



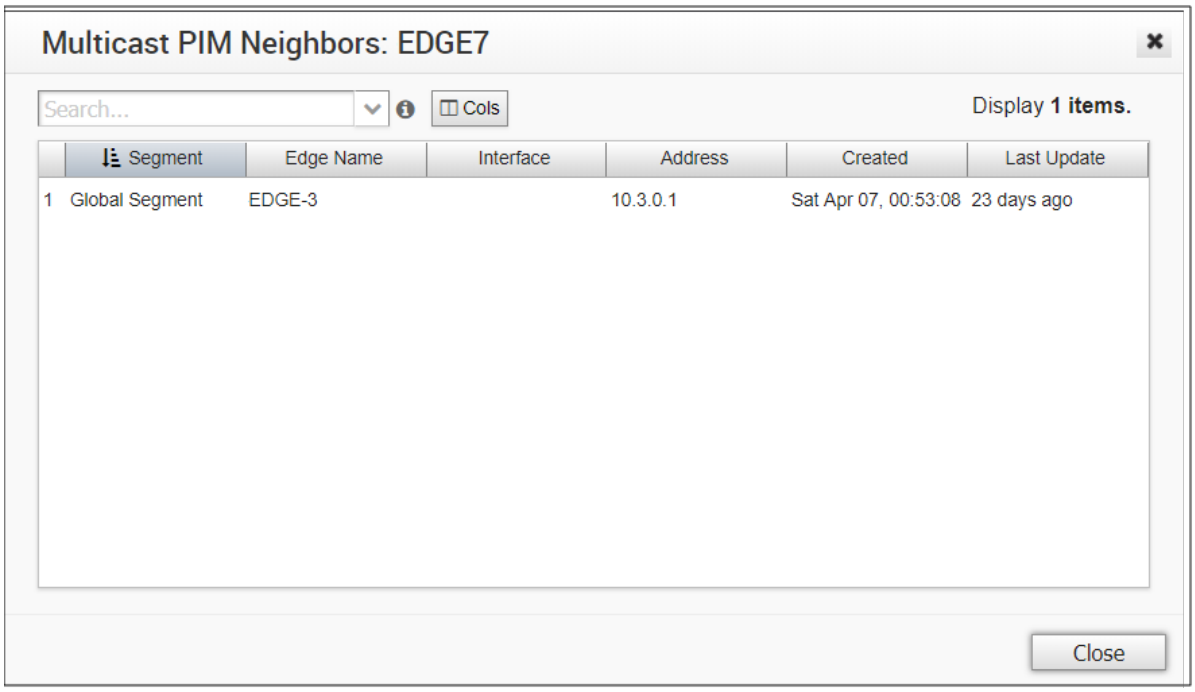
Überwachen des Routings

Die Routing-Funktion (Registerkarte **Überwachen > Routing > Multicast (Monitor > Routing > Multicast)**) zeigt Multicast-Gruppen- und Multicast-Edge-Informationen an.



Ansicht „PIM-Nachbarn“ (PIM Neighbors)

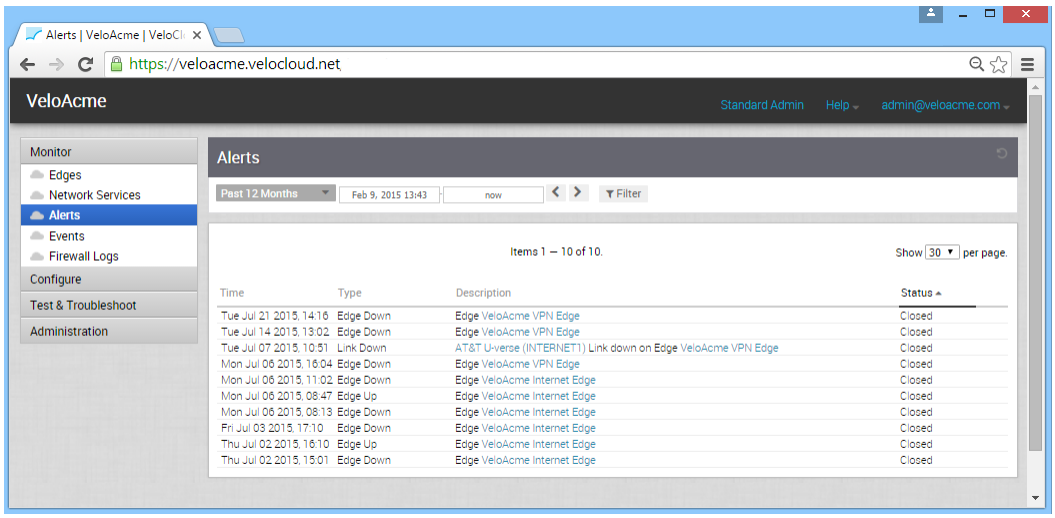
Die folgende Abbildung zeigt die PIM-Nachbarn des ausgewählten Edge (pro Segment), die Schnittstelle, in der der PIM-Nachbar erkannt wurde, die IP-Adresse des Nachbarn und die Zeitstempel.



Überwachen von Warnungen

SD-WAN Orchestrator bietet eine Warnungsfunktion, um einen oder mehrere Enterprise-Administratoren (oder andere Support-Benutzer) zu benachrichtigen, wenn ein Problem auftritt. Sie können auf diese Funktion zugreifen, indem Sie im Navigationsbereich unter **Überwachen (Monitor)** auf **Warnungen (Alerts)** klicken.

Sie können Warnungen senden, wenn ein SD-WAN Edge offline oder wieder online geschaltet wird, eine WAN-Verbindung ausfällt, ein VPN-Tunnel ausfällt oder ein Edge-HA-Failover auftritt. Für jeden der Warnungstypen kann eine Verzögerung für das Versenden der Warnung nach deren Erkennung eingegeben werden. Warnungen können Sie unter **Konfigurieren > Warnungen und Benachrichtigungen (Configure > Alerts and Notifications)** konfigurieren.

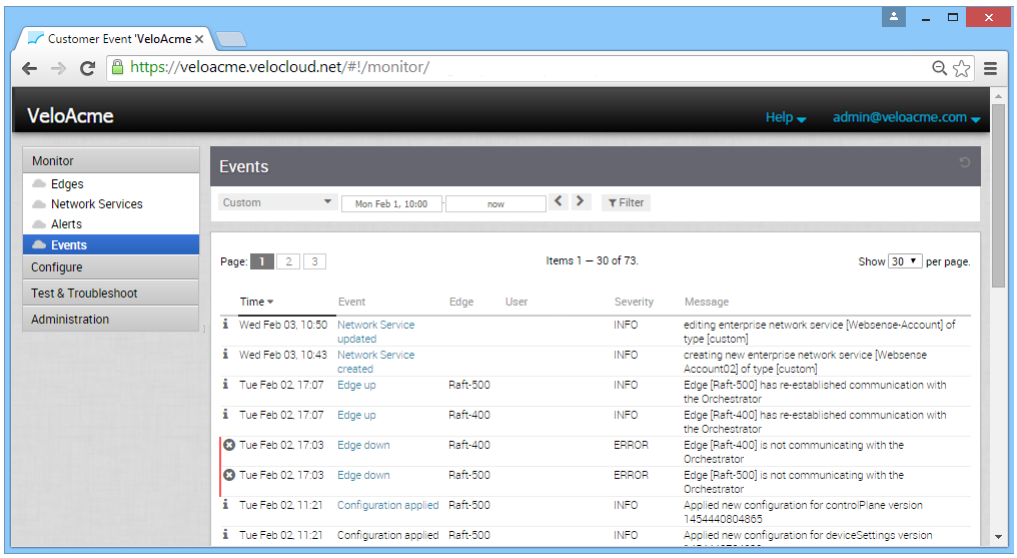


Hinweis Wenn Sie mit einer Benutzer-ID angemeldet sind, die über Kundensupport-Berechtigungen verfügt, können Sie nur SD-WAN Orchestrator-Objekte anzeigen. Sie werden nicht in der Lage sein, neue Objekte zu erstellen oder bestehende zu konfigurieren/aktualisieren.

Überwachen von Ereignissen

Auf der Seite **Ereignisse (Events)** im Navigationsbereich werden die vom SD-WAN Orchestrator erzeugten Ereignisse angezeigt. Mithilfe dieser Ereignisse können Sie den Betriebsstatus des VMware SD-WAN-Systems angeben.

Sie können auf den Link eines auf der Seite **Ereignisse (Events)** angezeigten Ereignis-Links klicken, um weitere Details anzuzeigen.



Die Funktion „Ereignisse (Events)“ eignet sich zum Abrufen der folgenden Informationen:

- Audit-Trail der Benutzeraktivität [Nach Benutzer filtern]
- Historischer Datensatz der Aktivitäten an einer bestimmten Site [Nach Site filtern]

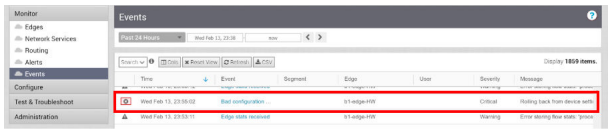
- Aufzeichnung von Ausfällen und signifikanten Netzwerkereignissen [Nach Ereignis filtern]
- Analyse der herabgestuften ISP-Leistung [Nach Zeitraum filtern]

Durchführen eines automatischen Rollback auf die letzte bekannte fehlerfreie Konfiguration

Wenn ein Administrator Gerätekonfigurationen ändert, die dazu führen, dass der Edge die Verbindung zum Orchestrator unterbricht, erhält der Administrator eine **Edge nicht aktiv (Edge Down)**-Warnung. Sobald der Edge erkennt, dass er die SD-WAN Orchestrator-Instanz nicht erreichen kann, führt er ein Rollback auf die letzte bekannte Konfiguration aus und erzeugt im Orchestrator ein Ereignis mit dem Titel „fehlerhafte Konfiguration (bad configuration)“.

Die Rollback-Zeit, d. h. die Zeit, die erforderlich ist, um eine fehlerhafte Konfiguration zu erkennen und die vorherige bekannte „fehlerfreie“ Konfiguration für einen eigenständigen Edge anzuwenden, beträgt 5-6 Minuten. Für HA-Edges beträgt die Rollback-Zeit 10-12 Minuten.

Hinweis Diese Funktion wird nur für Geräteeinstellungen auf der Edge-Ebene verwendet. Wenn die Konfiguration aus dem Profil entfernt wird, was dazu führt, dass mehrere Edges der Orchestrator-Instanz in den Offline-Modus wechseln, protokollieren die Edges „Fehlerhafte Konfigurationen (Bad Configuration)“-Ereignisse und führen ein Rollback auf die letzte bekannte fehlerfreie Konfiguration einzeln aus. WICHTIG: Der Administrator ist dafür verantwortlich, das Profil entsprechend festzulegen. Die Profilkonfiguration wird nicht automatisch zurückgesetzt.



Unterstützte VMware SD-WAN Edge-Ereignisse

In der folgenden Tabelle werden alle möglichen VMware SD-WAN Edge-Ereignisse beschrieben, die nach Syslog-Collector exportiert werden können.

Ereignisse	Schweregrad	Beschreibung
BW_UNMEASURABLE	WARNUNG	Wird von einem SD-WAN Edge generiert, wenn die Pfadbandbreite nicht messbar ist.
EDGE_BIOS_UPDATE_FAILED	FEHLER	Wird vom 12-upgrade-bios.sh- Skript generiert, wenn SD-WAN Edge BIOS aktualisiert wird.
EDGE_BIOS_UPDATED	INFO	Wird vom 12-upgrade-bios.sh-Skript generiert, wenn das SD-WAN Edge BIOS-Update fehlgeschlagen ist.
EDGE_COMMAND	INFO	Wird von einem SD-WAN Edge während der Remote-Diagnose bei der Ausführung von Edge-Befehlen generiert.

Ereignisse	Schweregrad	Beschreibung
EDGE_CONSOLE_LOGIN	INFO	Wird von einem SD-WAN Edge während der Anmeldung über den Konsolenport generiert.
EDGE_DEACTIVATED	WARNUNG	Wird generiert, wenn die gesamte Konfiguration eines SD-WAN Edge gelöscht wird und der Edge nicht mit einer Kunden-Site verknüpft ist. Der Software-Build bleibt unverändert.
EDGE_DHCP_BAD_OPTION	WARNUNG	Wird generiert, wenn der SD-WAN Edge mit einer ungültigen DHCP-Option konfiguriert wird.
EDGE_DISK_IO_ERROR	WARNUNG	Wird von einem SD-WAN Edge generiert, wenn ein Festplatten-E/A-Fehler beim Upgrade/Downgrade aufgetreten ist.
EDGE_DISK_READONLY	KRITISCH	Wird durch einen SD-WAN Edge generiert, wenn eine Festplatte in den schreibgeschützten Modus wechselt.
EDGE_DNSMASQ_FAILED	FEHLER	Wird generiert, wenn der Dnsmasq-Dienst fehlgeschlagen ist.
EDGE_DOT1X_SERVICE_DISABLED	WARNUNG, KRITISCH	Wird von vc_procmon generiert, wenn der 802.1x-Dienst des SD-WAN Edge deaktiviert ist.
EDGE_DOT1X_SERVICE_FAILED	FEHLER	Wird von vc_procmon generiert, wenn der 802.1x-Dienst des SD-WAN Edge fehlschlägt.
EDGE_HARD_RESET	WARNUNG	Wird generiert, wenn der Benutzer einen Kaltstart für SD-WAN Edge initiiert hat.
EDGE_HEALTH_ALERT	NOTFALL	Wird vom SD-WAN Edge generiert, wenn die Datenebene nicht in der Lage ist, notwendige Ressourcen für die Paketverarbeitung zuzuweisen.
EDGE_INTERFACE_DOWN	INFO	Wird von Hotplug-Skripten generiert, wenn die Schnittstelle nicht verfügbar ist.
EDGE_INTERFACE_UP	INFO	Wird von Hotplug-Skripten generiert, wenn die Schnittstelle betriebsbereit ist.

Ereignisse	Schweregrad	Beschreibung
EDGE_KERNEL_PANIC	WARNUNG	Wird von einem SD-WAN Edge generiert, wenn das Edge-Betriebssystem auf eine kritische Ausnahme gestoßen ist und der Edge durch einen Neustart wiederhergestellt werden muss. Ein Edge-Neustart unterbricht den Kundendatenverkehr für 2–3 Minuten, bis der Edge-Neustart abgeschlossen ist.
EDGE_L2_LOOP_DETECTED	FEHLER	Wird generiert, wenn die L2-Schleife des SD-WAN Edge erkannt wird.
EDGE_LED_SERVICE_DISABLED	WARNUNG, KRITISCH	Wird von vc_procmon generiert, wenn der LED-Dienst des SD-WAN Edge deaktiviert ist.
EDGE_LED_SERVICE_FAILED	FEHLER	Wird von vc_procmon generiert, wenn der LED-Dienst des SD-WAN Edge fehlgeschlagen ist.
EDGE_LOCALUI_LOGIN	INFO	Wird generiert, wenn die Anmeldung über die LOKALE Benutzerschnittstelle für einen Benutzer erfolgreich ist.
EDGE_MEMORY_USAGE_ERROR	FEHLER	Wird von einem SD-WAN Edge generiert, wenn der Ressourcenüberwachungsprozess feststellt, dass die Edge-Speicherauslastung definierte Schwellenwerte überschritten hat und einen Schwellenwert von 70 % erreicht. Die Ressourcenüberwachung wartet 90 Sekunden lang, damit sich der Edge-Prozess von einer möglichen temporären Spitze der Arbeitsspeichernutzung erholen kann. Wenn die Arbeitsspeichernutzung für mehr als 90 Sekunden auf einem Wert von 70 % oder höher anhält, generiert der Edge diese Fehlermeldung und sendet dieses Ereignis an den Orchestrator.
EDGE_MEMORY_USAGE_WARNING	WARNUNG	Wird von einem SD-WAN Edge generiert, wenn der Ressourcenüberwachungsprozess feststellt, dass die Edge-Arbeitsspeicherauslastung mindestens 50 % des verfügbaren Arbeitsspeichers beträgt. Dieses Ereignis wird alle 60 Minuten an den Orchestrator gesendet, bis die Arbeitsspeichernutzung unter den Schwellenwert von 50 % sinkt.

Ereignisse	Schweregrad	Beschreibung
EDGE_MGD_SERVICE_DISABLED	KRITISCH, WARNUNG	Wird von vc_procmon generiert, wenn mgd aufgrund zu vieler Fehler nicht gestartet oder deaktiviert werden kann.
EDGE_MGD_SERVICE_FAILED	FEHLER	Wird von vc_procmon generiert, wenn der mgd-Dienst fehlgeschlagen ist.
EDGE_NEW_DEVICE	INFO	Wird generiert, wenn ein neuer DHCP-Client durch die Verarbeitung der DHCP-Anforderung identifiziert wird.
EDGE_NEW_USER	INFO	Wird generiert, wenn ein neuer Clientbenutzer hinzugefügt wird.
EDGE_OSPF_NSM	INFO	Wird vom SD-WAN Edge generiert, wenn der Status OSPF Neighbor State Machine (NSM) aufgetreten ist.
EDGE_REBOOTING	WARNUNG	Wird generiert, wenn ein Benutzer einen Neustart des SD-WAN Edge initiiert hat.
EDGE_RESTARTING	WARNUNG	Wird generiert, wenn ein Benutzer einen Neustart des SD-WAN Edge-Diensts initiiert hat.
EDGE_SERVICE_DISABLED	WARNUNG	Wird generiert, wenn der SD-WAN Edge-Datenebenendienst deaktiviert wird.
EDGE_SERVICE_ENABLED	WARNUNG	Wird generiert, wenn der SD-WAN Edge-Datenebenendienst aktiviert wird.
EDGE_SERVICE_FAILED	FEHLER	Wird generiert, wenn der SD-WAN Edge-Datenebenendienst fehlgeschlagen ist.
EDGE_SHUTTING_DOWN	WARNUNG	Wird generiert, wenn ein SD-WAN Edge heruntergefahren wird.
EDGE_STARTUP	INFO	Wird generiert, wenn ein SD-WAN Edge im reinen Verwaltungsmodus ausgeführt wird.
EDGE_SSH_LOGI	INFO	Wird von einem SD-WAN Edge bei der Anmeldung über das SSH-Protokoll generiert.
EDGE_TUNNEL_CAP_WARNING	WARNUNG	Wird generiert, wenn ein SD-WAN Edge seine maximale Tunnelkapazität erreicht hat.
EDGE_VNFD_SERVICE_DISABLED	WARNUNG, KRITISCH	Wird von vc_procmon generiert, wenn der VNFD-Dienst des Edge deaktiviert wird.

Ereignisse	Schweregrad	Beschreibung
EDGE_VNFD_SERVICE_FAILED	FEHLER	Wird von vc_procmon generiert, wenn der VNFD-Dienst des Edge fehlgeschlagen ist.
FLOOD_ATTACK_DETECTED	INFO	Wird generiert, wenn ein böswilliger Host den SD-WAN Edge mit neuen Verbindungen überflutet (Flood-Angriff).
HA_FAILED	INFO	HA-Peer-Status unbekannt: Wird erzeugt, wenn der Standby-Edge keine Taktsignal-Antwort gesendet hat und nur einer der beiden HA-Edges mit dem Orchestrator und den Gateways kommuniziert.
HA_GOING_ACTIVE	INFO	Ein HA-Failover. Wird generiert, wenn der aktive Hochverfügbarkeits (HA)-Edge als nicht verfügbar markiert wurde und der Standby-Edge in den aktiven Status versetzt wird.
HA_INTF_STATE_CHANGED	WARNUNG	Wird generiert, wenn die HA-Schnittstelle in den aktiven Status versetzt wird.
HA_READY	INFO	Wird generiert, wenn der aktive und der Standby-Edge beide verfügbar sind und synchronisiert werden.
HA_STANDBY_ACTIVATED	INFO	Wird generiert, wenn der HA-Standby-Edge den Aktivierungsschlüssel akzeptiert, die Konfiguration heruntergeladen und den Software-Build aktualisiert hat.
HA_TERMINATED	INFO	Wird generiert, wenn HA auf einem SD-WAN Edge deaktiviert wurde.
INVALID_JSON	KRITISCH	Wird generiert, wenn ein SD-WAN Edge eine ungültige Antwort von MGD empfangen hat.
IP_SLA_PROBE	Verfügbar = INFO, Nicht verfügbar = WARNUNG	Wird bei einem Statuswechsel des IP-ICMP-Tests generiert.
IP_SLA_RESPONDER	Verfügbar = INFO, Nicht verfügbar = WARNUNG	Wird bei einem Statuswechsel des IP-ICMP-Responders generiert.
LINK_ALIVE	INFO	Wird generiert, wenn ein WAN-Link nicht mehr INAKTIV ist.
LINK_DEAD	WARNUNG	Wird generiert, wenn alle auf dem WAN-Link eingerichteten Tunnel mindestens sieben Sekunden lang keine Pakete empfangen haben.

Ereignisse	Schweregrad	Beschreibung
LINK_MTU	INFO	Wird generiert, wenn die MTU des WAN-Links ermittelt wird.
LINK_UNUSABLE	WARNUNG	Wird generiert, wenn der WAN-Link in einen NICHT VERWENDBAREN Status übergeht.
LINK_USABLE	INFO	Wird generiert, wenn der WAN-Link in einen VERWENDBAREN Status übergeht.
MGD_ACTIVATION_ERROR	FEHLER	Wird generiert, wenn eine SD-WAN Edge-Aktivierung fehlgeschlagen ist. Entweder war der Aktivierungslink nicht korrekt oder die Konfiguration wurde nicht korrekt auf den Edge heruntergeladen.
MGD_ACTIVATION_PARTIAL	INFO	Wird generiert, wenn ein SD-WAN Edge teilweise aktiviert wird, aber eine Softwareaktualisierung fehlgeschlagen ist.
MGD_ACTIVATION_SUCCESS	INFO	Wird generiert, wenn ein SD-WAN Edge erfolgreich aktiviert wurde.
MGD_CONF_APPLIED	INFO	Wird generiert, wenn eine am Orchestrator vorgenommene Konfigurationsänderung an den SD-WAN Edge verschoben wurde und erfolgreich angewendet wird.
MGD_CONF_FAILED	INFO	Wird generiert, wenn der SD-WAN Edge eine am Orchestrator vorgenommene Konfigurationsänderung nicht anwenden konnte.
MGD_CONF_ROLLBACK	INFO	Wird generiert, wenn eine vom Orchestrator gesendete Konfigurationsrichtlinie zurückgerollt werden musste, weil sie der SD-WAN Edge destabilisiert hat.
MGD_CONF_UPDATE_INVALID	INFO	Wird generiert, wenn einem SD-WAN Edge ein Operator-Profil mit einem ungültigen Software-Image zugewiesen wurde, das der Edge nicht verwenden kann.
MGD_DEACTIVATED	INFO	Wird generiert, wenn ein SD-WAN Edge basierend auf einer Benutzeranforderung von mgd deaktiviert wird.

Ereignisse	Schweregrad	Beschreibung
MGD_DEVICE_CONFIG_WARNING/ ERROR	WARNUNG, INFO	Wird generiert, wenn eine inkonsistente/ungültige Geräteeinstellung erkannt wird.
MGD_DIAG_REBOOT	INFO	Wird generiert, wenn ein SD-WAN Edge von einer Remote-Aktion aus dem Orchestrator neu gestartet wird.
MGD_DIAG_RESTART	INFO	Wird generiert, wenn der Datenebenendienst auf dem SD-WAN Edge von einer Remote-Aktion aus dem Orchestrator neu gestartet wird.
MGD_EMERG_REBOOT	KRITISCH	Wird generiert, wenn ein SD-WAN Edge neu durch vc_procmon neu gestartet wird, um sie von festgefahrenen Prozessen wiederherzustellen.
MGD_ENTER_LIVE_MODE	DEBUGGEN	Wird generiert, wenn der Verwaltungsdienst auf einem SD-WAN Edge in den LIVE-Modus wechselt.
MGD_EXIT_LIVE_MODE	DEBUGGEN	Wird generiert, wenn der Verwaltungsdienst auf einem SD-WAN Edge den LIVE-Modus beendet.
MGD_EXITING	INFO	Wird generiert, wenn der Verwaltungsdienst auf einem SD-WAN Edge für einen Neustart heruntergefahren wird.
MGD_EXTEND_LIVE_MODE	DEBUGGEN	Wird durch einen SD-WAN Edge generiert, wenn der Live-Modus erweitert wird.
MGD_FLOW_STATS_PUSH_FAILED	DEBUGGEN	Wird von einem SD-WAN Edge generiert, wenn die Flow-Statistik zu Orchestrator verschoben wurde.
MGD_FLOW_STATS_PUSH_SUCCEED ED	DEBUGGEN	Wird von einem SD-WAN Edge generiert, wenn die Verschiebung der Flow-Statistik zu Orchestrator erfolgreich war.
MGD_FLOW_STATS_QUEUED	INFO	Wird von einem SD-WAN Edge generiert, wenn die Verschiebung der Flow-Statistik zu Orchestrator in die Warteschlange gestellt wird.
MGD_HARD_RESET	INFO	Wird generiert, wenn ein SD-WAN Edge auf seine werkseitige Software und Konfiguration zurückgesetzt wird.

Ereignisse	Schweregrad	Beschreibung
MGD_HEALTH_STATS_PUSH_FAILED	DEBUGGEN	Wird von einem SD-WAN Edge generiert, wenn das Verschieben der Integritätsstatistik zu Orchestrator fehlgeschlagen ist.
MGD_HEALTH_STATS_PUSH_SUCCEEDED	DEBUGGEN	Wird von einem SD-WAN Edge generiert, wenn das Verschieben der Integritätsstatistik zu Orchestrator erfolgreich war.
MGD_HEALTH_STATS_QUEUED	INFO	Wird von einerm SD-WAN Edge generiert, wenn die Verschiebung der Integritätsstatistik zu Orchestrator in die Warteschlange gestellt wird.
MGD_HEARTBEAT	INFO	Wird von einem SD-WAN Edge generiert, wenn Taktsignale an Orchestrator generiert werden.
MGD_HEARTBEAT_FAILURE	INFO	Wird von einem SD-WAN Edge generiert, wenn das Generieren von Taktsignalen an Orchestrator fehlgeschlagen ist.
MGD_HEARTBEAT_SUCCESS	INFO	Wird von einem SD-WAN Edge generiert, wenn das Generieren von Taktsignalen an Orchestrator erfolgreich war.
MGD_INVALID_VCO_ADDRESS	WARNUNG	Wird generiert, wenn eine ungültige Adresse für Orchestrator in einer Richtlinienaktualisierung der Verwaltungsebene gesendet und ignoriert wurde.
MGD_LINK_STATS_PUSH_FAILED	DEBUGGEN	Wird von einem SD-WAN Edge generiert, wenn das Verschieben der Link-Statistik zu Orchestrator fehlgeschlagen ist.
MGD_LINK_STATS_PUSH_SUCCEEDED	DEBUGGEN	Wird von einem SD-WAN Edge generiert, wenn das Verschieben der Link-Statistik zu Orchestrator erfolgreich war.
MGD_LINK_STATS_QUEUED	INFO	Wird von einem SD-WAN Edge generiert, wenn die Verschiebung der Link-Statistik zu Orchestrator in die Warteschlange gestellt wird.
MGD_LIVE_ACTION_FAILED	DEBUGGEN	Wird von einem SD-WAN Edge generiert, wenn die Live-Aktion fehlgeschlagen ist.
MGD_LIVE_ACTION_REQUEST	DEBUGGEN	Wird von einem SD-WAN Edge generiert, wenn die Live-Aktion angefordert wird.

Ereignisse	Schweregrad	Beschreibung
MGD_LIVE_ACTION_SUCCEEDED	DEBUGGEN	Wird von einem SD-WAN Edge generiert, wenn die Live-Aktion erfolgreich war.
MGD_NETWORK_MGMT_IF_BROKEN	WARNUNG	Wird generiert, wenn das Verwaltungsnetzwerk falsch eingerichtet ist.
MGD_NETWORK_MGMT_IF_FIXED	WARNUNG	Wird generiert, wenn ein Netzwerk zweimal neu gestartet wird, um die Inkonsistenz des Verwaltungsnetzwerks zu beheben.
MGD_NETWORK_SETTINGS_UPDATED	INFO	Wird generiert, wenn neue Netzwerkeinstellungen auf einen SD-WAN Edge angewendet werden.
MGD_SET_CERT_FAIL	FEHLER	Wird generiert, wenn die Installation eines neuen PKI-Zertifikats für die VCO-Kommunikation auf einem SD-WAN Edge fehlgeschlagen ist.
MGD_SET_CERT_SUCCESS	INFO	Wird generiert, wenn ein neues PKI-Zertifikat für die VCO-Kommunikation erfolgreich auf einem SD-WAN Edge installiert wird.
MGD_SHUTDOWN	INFO	Wird generiert, wenn die SD-WAN Edge-Diagnose aufgrund einer Benutzeranforderung heruntergefahren wurde.
MGD_START	INFO	Wird generiert, wenn der Verwaltungsdaemon auf dem SD-WAN Edge gestartet wurde.
MGD_SWUP_DOWNLOAD_FAILED	FEHLER	Wird generiert, wenn der Download eines Image für die Aktualisierung der Edge-Software fehlgeschlagen ist.
MGD_SWUP_DOWNLOAD_SUCCEEDED	DEBUGGEN	Wird generiert, wenn der Download eines Image für die Aktualisierung der Edge-Software erfolgreich war.
MGD_SWUP_IGNORED_UPDATE	INFO	Wird generiert, wenn ein Software-Update zum Aktivierungszeitpunkt ignoriert wird, da der SD-WAN Edge diese Version bereits ausführt.
MGD_SWUP_INSTALL_FAILED	FEHLER	Wird generiert, wenn die Installation eines Software-Updates fehlgeschlagen ist.
MGD_SWUP_INSTALLED	INFO	Wird generiert, wenn ein Software-Update erfolgreich heruntergeladen und installiert wurde.

Ereignisse	Schweregrad	Beschreibung
MGD_SWUP_INVALID_SWUPDATE	WARNUNG	Wird generiert, wenn ein vom Orchestrator empfangenes Software-Updatepaket ungültig ist.
MGD_SWUP_REBOOT	INFO	Wird generiert, wenn der SD-WAN Edge nach einem Software-Update neu gestartet wird.
MGD_SWUP_STANDBY_UPDATE_FAILED	FEHLER	Wird generiert, wenn ein Software-Update des Standby-HA-Edge fehlgeschlagen ist.
MGD_SWUP_STANDBY_UPDATE_START	INFO	Wird generiert, wenn das Software-Update für Standby-HA gestartet wurde.
MGD_SWUP_STANDBY_UPDATED	INFO	Wird generiert, wenn ein Software-Update des Standby-HA-Edge abgeschlossen wurde.
MGD_SWUP_UNPACK_FAILED	FEHLER	Wird generiert, wenn ein Edge das heruntergeladene Software-Updatepaket nicht entpackt hat.
MGD_SWUP_UNPACK_SUCCEEDED	INFO	Wird generiert, wenn ein Edge das heruntergeladene Software-Updatepaket erfolgreich entpackt hat.
MGD_UNREACHABLE	NOTFALL	Wird generiert, wenn der Prozess der Datenebene nicht mit dem Proxy der Verwaltungsebene kommunizieren konnte.
MGD_VCO_ADDR_RESOLV_FAILED	WARNUNG	Wird generiert, wenn die DNS-Auflösung der Orchestrator-Adresse fehlgeschlagen ist.
MGD_WEBSOCKET_INIT	DEBUGGEN	Wird generiert, wenn eine WebSocket-Kommunikation mit dem Orchestrator initiiert wird.
MGD_WEBSOCKET_CLOSE	DEBUGGEN	Wird generiert, wenn eine WebSocket-Kommunikation mit dem Orchestrator geschlossen wird.
PEER_UNUSABLE	WARNUNG	Wird generiert, wenn die Overlay-Konnektivität zu einem Peer nicht mehr verfügbar ist, während Peer-Statistiken übertragen werden.
PEER_USABLE	INFO	Wird generiert, wenn die Overlay-Konnektivität zu einem Peer nach einem Ausfall wiederaufgenommen wird.
PORT_SCAN_DETECTED	INFO	Wird generiert, wenn der Port-Scan erkannt wird.

Ereignisse	Schweregrad	Beschreibung
QOS_OVERRIDE	INFO	Wird generiert, um den Datenverkehrspfad (Gateway oder direkt) umzukehren.
SLOW_START_CAP_MET	HINWEIS	Wird generiert, wenn der Grenzwert für den Langsam-Start der Bandbreitenmessung überschritten wird. Dieser Vorgang wird im Burstmodus ausgeführt.
VPN_DATACENTER_STATUS	INFO, FEHLER	Wird bei einem Statuswechsel eines VPN-Tunnels generiert.
VRRP_FAIL_INFO	INFO	Wird generiert, wenn VRRP fehlgeschlagen ist.
VRRP_INTO_MASTER_STATE	INFO	Wird generiert, wenn VRRP in den Master-Status übergeht.
VRRP_OUT_OF_MASTER_STATE	INFO	Wird generiert, wenn VRRP aus dem Master-Status herauskommt.

Überwachen von Berichten

Das Überwachungs-Dashboard im Unternehmensportal ermöglicht das Erstellen von Berichten mit der Gesamtübersicht des Netzwerks sowie Informationen zu SD-WAN-Datenverkehr und -Transportverteilung. Die Berichte ermöglichen die Analyse Ihres Netzwerks.

Hinweis Schwerpunkt der Berichte liegt auf deskriptiven Analysen. Sie können nicht für die Fehlerbehebung verwendet werden. Darüber hinaus handelt es sich bei diesen Berichten nicht um Dashboards, die die Echtzeitdaten aus dem Netzwerk widerspiegeln.

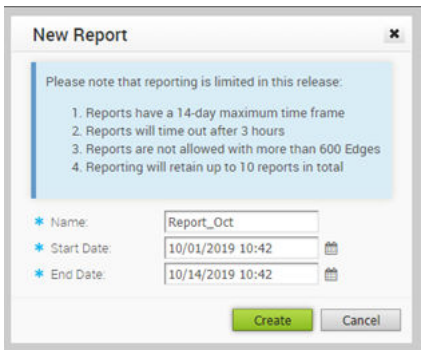
Klicken Sie im Unternehmensportal auf **Überwachen (Monitor) > Berichte (Reports)**.

So erstellen Sie einen neuen Bericht:

1 Klicken Sie im Fenster **Berichte (Reports)** auf **Neuer Bericht (New Report)**.

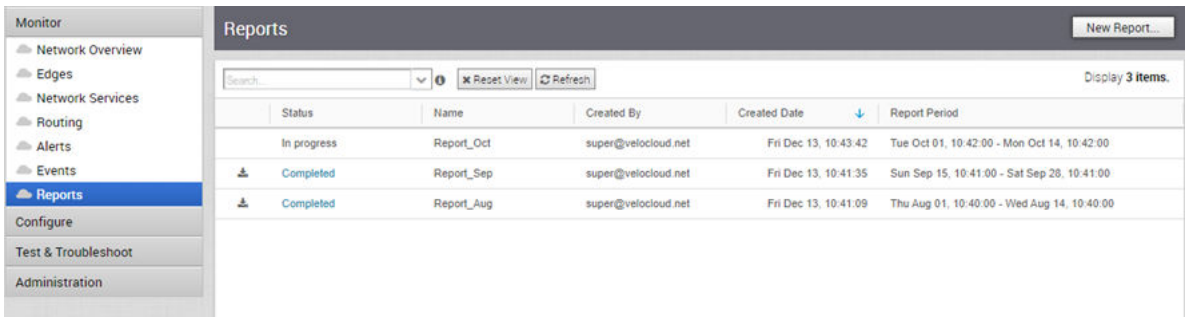
2 Geben Sie im Fenster **Neuer Bericht (New Report)** einen beschreibenden Namen für den Bericht ein und wählen Sie das Anfangs- und Enddatum aus.

3 Klicken Sie auf **Erstellen (Create)**.



Hinweis Sie können einen Bericht nur für eine Dauer von 14 Tagen und für maximal 600 Edges erstellen. Bei der Berichterstellung kommt es nach 3 Stunden zu einem Timeout. In der Tabelle **Berichte (Reports)** werden immer nur die letzten 10 Berichte beibehalten.

Der **Status** der Berichterstellung wird im Fenster angezeigt. Nachdem der Bericht erstellt wurde, können Sie ihn herunterladen, indem Sie auf den Link **Abgeschlossen (Completed)** klicken.



Das Fenster **Bericht herunterladen (Download Report)** bietet die folgenden Optionen:

Sie können den Bericht als PDF herunterladen, der eine Gesamtübersicht über die Datenverkehrs- und Transportverteilung, dargestellt als Kreisdiagramm, enthält. Dieser Bericht enthält auch die Liste der 10 wichtigsten Anwendungen nach Datenverkehr und Transporttyp.

Sie können die Berichte nach Transport- oder Datenverkehrsverteilung als CSV-Datei herunterladen.

- Der Bericht zur Transportverteilung zeigt die Details zu Zeit, Transportart, Anwendungen, Name und Beschreibung der Edges sowie die gesendeten und empfangenen Byte an.
- Der Bericht zur Datenverkehrsverteilung zeigt die Details zu Zeit, Flow-Pfad, Anwendungen, Name und Beschreibung der Edges sowie die gesendeten und empfangenen Byte an.

Konfigurieren von Segmenten 7

Bei der Segmentierung wird das Netzwerk in als Segmente bezeichnete logische Subnetzwerke unterteilt, indem Isolierungstechniken auf einem Weiterleitungsgerät, wie z. B. einem Switch, Router oder einer Firewall, verwendet werden. Netzwerksegmentierung ist wichtig, wenn Datenverkehr aus verschiedenen Organisationen und/oder Datentypen isoliert werden muss.

In der segmentfähigen Topologie können verschiedene VPN-Profile (Virtual Private Network) für jedes Segment aktiviert werden. Beispielsweise kann der Gastdatenverkehr zu den Firewalldiensten des Remote-Datencenters zurückgeschickt werden, Sprachmedien können auf der Grundlage dynamischer Tunnel direkt von Branch zu Branch fließen, und das PCI-Segment kann den Datenverkehr zum Datencenter zurückverlagern, um das PCI-Netzwerk zu verlassen.

Hinweis Sie können maximal 16 Segmente pro Unternehmenskunde konfigurieren.

Führen Sie die folgenden Schritte aus, um ein neues Segment für ein Unternehmen zu konfigurieren:

1 Wechseln Sie im Navigationsbereich von SD-WAN Orchestrator zu **Konfigurieren (Configure) > Segmente (Segments)**. Die Seite **Segmente (Segments)** wird für das ausgewählte Unternehmen angezeigt.

2 Klicken Sie auf die Schaltfläche **+** und geben Sie die folgenden Details zum Konfigurieren eines neuen Segments ein.

Feld	Beschreibung
Segmentname (Segment Name)	Der Name des Segments (bis zu 256 Zeichen).
Beschreibung (Description)	Die Beschreibung des Segments (bis zu 256 Zeichen).

Feld	Beschreibung
Typ (Type)	Folgende Segmenttypen stehen zur Verfügung: ■ **Regulär (Regular)** – Der Standardsegmenttyp. ■ **Privat (Private)** – Wird für Datenverkehrsströme mit beschränkter Sichtbarkeit verwendet, um den Datenschutzanforderungen der Endbenutzer Rechnung zu tragen. ■ **CDE** – VMware SD-WAN Bietet einen PCI-zertifizierten SD-WAN-Dienst. Der CDE-Typ (Cardholder Data Environment) wird für Datenverkehrsströme verwendet, die PCI benötigen und die VMware SD-WAN-PCI-Zertifizierung nutzen möchten. **Hinweis** Für globale Segmente können Sie den Typ entweder auf **Regulär (Regular)** oder **Privat (Private)** festlegen. Für nicht globale Segmente kann **Regulär (Regular)**, **CDE** oder **Privat (Private)** als Typ verwendet werden.
Dienst-VLAN (Service VLAN)	Der VLAN-Bezeichner des Diensts. Weitere Informationen finden Sie im Abschnitt *Definieren der Zuordnung zwischen Segmenten und Dienst-VLANs (optional)* in Sicherheits-VNFs.
An Partner delegieren (Delegate To Partner)	Dieses Kontrollkästchen ist standardmäßig aktiviert. Wenn Sie es deaktivieren, kann der Partner die Konfigurationen innerhalb des Segments, einschließlich der Schnittstellenzuweisung, nicht ändern.
An Kunden delegieren (Delegate To Customer)	Dieses Kontrollkästchen ist standardmäßig aktiviert. Wenn Sie es deaktivieren, kann der Kunde die Konfigurationen innerhalb des Segments, einschließlich der Schnittstellenzuweisung, nicht ändern.

3 Klicken Sie auf **Änderungen speichern (Save Changes)**.

Die Konfiguration des Segments als **Privat (Private)** hat folgende Auswirkungen:

- Das Segment kann keine Flow-Statistiken des Benutzers in VCO hochladen, ausgenommen VMware SD-WAN-Steuerung, VMware SD-WAN-Verwaltung und eines einzelnen IP-Flusses, der alle übertragenen und empfangenen Pakete und Byte für das Segment zählt.
- Benutzer können keine Flows in Remote Diagnostics anzeigen.
- Datenverkehr darf nicht als **Internet Multipath** gesendet werden, da alle an **Internet Multipath** gesendeten Geschäftsrichtlinien automatisch vom Edge in **Direkt (Direct)** überschrieben werden.

Wenn das Segment als **CDE** konfiguriert ist, kennen der von VMware SD-WAN gehostete Orchestrator und Controller das PCI-Segment und gehören zum PCI-Geltungsbereich. Gateways (die als Nicht-CDE-Gateways gekennzeichnet sind) erkennen oder übermitteln den PCI-Datenverkehr nicht und befinden sich nicht im PCI-Geltungsbereich.

Konfigurieren von Netzwerkdiensten

8

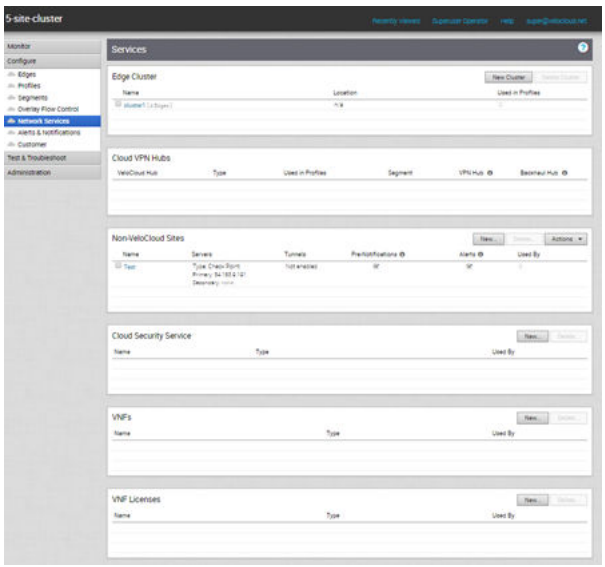
Als Unternehmenskunde ermöglicht Ihnen SD-WAN Orchestrator die Konfiguration von Netzwerkdiensten über **Konfigurieren (Configure)** > **Netzwerkdienste (Network Services)**.

Hinweis Wenn Sie mit einer Benutzer-ID angemeldet sind, die über Kundensupport-Berechtigungen verfügt, können Sie nur SD-WAN Orchestrator-Objekte anzeigen. Sie werden nicht in der Lage sein, neue Objekte zu erstellen oder bestehende zu konfigurieren/aktualisieren.

Sie können die folgenden Netzwerkdienste konfigurieren:

- Edge-Cluster
- Nicht-VeloCloud-Sites
- Cloud-Sicherheitsdienst
- VNFs
- VNF-Lizenzen
- DNS-Dienste
- NetFlow-Einstellungen
- Private Netzwerknamen
- Authentifizierungsdienste

Hinweis Das Konfigurieren von Netzwerkdiensten ist optional und kann in beliebiger Reihenfolge konfiguriert werden.



Hinweis SD-WAN Orchestrator lässt nicht zu, dass die Cloud-VPN-Hubs über den Bildschirm **Dienste (Services)** konfiguriert werden, stellt aber eine Zusammenfassung aller konfigurierten SD-WAN Edges-Instanzen bereit. Die Zusammenfassung enthält Folgendes: Edge-Typ, Profil, in dem der Edge verwendet wird, Segment sowie Angaben dazu, ob es sich bei dem Edge um einen VPN-Hub oder/und einen Backhaul-Hub handelt.

Dieses Kapitel enthält die folgenden Themen:

Info zu Edge-Clustering

Die Größe eines einzelnen VMware SD-WAN-VPN-Netzwerks mit einem VMware SD-WAN Hub wird durch die Größe des einzelnen Hubs begrenzt. Bei großen Netzwerken mit Tausenden von Remote-Sites empfiehlt sich aus Gründen der Skalierbarkeit und Risikominimierung die Verwendung mehrerer Hubs zur Verarbeitung der Edges. Dem Kunden zur Erreichung dieses Ziels die Verwaltung einzelner separater Hubs aufzuerlegen, erweist sich jedoch als nicht zweckmäßig. Clustering ermöglicht die Nutzung mehrerer Hubs und bietet gleichzeitig die einfache Verwaltung dieser Hubs als eine Einheit mit integrierter Ausfallsicherheit.

SD-WAN Edge-Clustering behebt das Problem der SD-WAN Hub-Skalierung, da mithilfe von Clustering die Tunnelkapazität des Hubs dynamisch erweitert werden kann, indem ein logischer Cluster aus Edges erstellt wird. Edge-Clustering bietet darüber hinaus Ausfallsicherheit über die Aktiv/Aktiv-HA-Topologie (High Availability), die in einem SD-WAN Edges-Cluster bereitsteht. Ein Cluster wird aus Sicht anderer Edges funktionell als einzelner Hub behandelt.

Bei den Hubs in einem VMware SD-WAN-Cluster kann es sich um physische oder virtuelle Edges handeln. Virtuelle Edges befinden sich unter Umständen auf einem einzelnen oder mehreren Hypervisoren.

Jeder Edge in einem Cluster meldet in regelmäßigen Abständen Nutzungs- und Laststatistiken an das SD-WAN Gateway. Der Lastwert wird basierend auf der CPU- und Arbeitsspeichernutzung des Edge sowie der Anzahl der mit dem Hub verbundenen Tunnel als Prozentsatz der Tunnelkapazität des Edge-Modells berechnet. Zwischen den Hubs im Cluster findet weder Kommunikation noch ein Austausch von Statusinformationen statt. In der Regel werden Edge-Cluster als Hubs in Datencentern bereitgestellt.

Hinweis Theoretisch könnte Edge-Clustering für die horizontale Skalierung anderer Vektoren verwendet werden, wie z. B. Durchsatz. Die aktuelle Edge-Clustering-Implementierung wurde jedoch speziell für die Skalierung der Tunnelkapazität konzipiert und getestet.

Funktionsweise von Edge-Clustering

Dieser Abschnitt bietet einen ausführlichen Überblick darüber, wie die SD-WAN Edge-Clustering-Funktion arbeitet.

Es gibt vier wichtige Konzepte, die vor der Beschreibung der SD-WAN Edge-Clustering-Funktionalität verstanden werden müssen.

1. Edge-Clustering wurde für den Einsatz auf Hubs wie folgt konzipiert und getestet:
   - Um eine größere Tunnelkapazität für einen Hub zu ermöglichen, als ein einzelner als Hub dienender Edge bieten kann.
   - Um die Remote-Spoke-Edges auf mehrere Hubs zu verteilen und die Auswirkungen eines eventuell auftretenden Zwischenfalls zu reduzieren.
2. Cluster Score ist eine mathematische Berechnung der Gesamtauslastung des Systems wie folgt:
   - Die drei gemessenen Auslastungsfaktoren sind CPU-Auslastung, Speichernutzung und Tunnelkapazität.
     - Jede Nutzungsmessung wird als Prozentsatz eines Maximums von 100 % behandelt.
     - Die Tunnelkapazität basiert auf der bewerteten Kapazität für ein bestimmtes Hardwaremodell oder eine Virtual Edge-Konfiguration.
     - Alle drei Nutzungsprozentsätze werden gemittelt, um einen ganzzahlbasierten Cluster Score (1 – 100) zu erhalten.

- Der Durchsatz wird zwar nicht direkt berücksichtigt, aber die Nutzung von CPU und Arbeitsspeicher spiegeln indirekt den Durchsatz und das Flow-Volumen auf einem bestimmten Hub wider.
- Beispielsweise auf einem Edge 2000:
  - CPU-Nutzung = 20 %
  - Arbeitsspeichernutzung = 30 %
  - Verbundene Tunnel = 600 (von 6000) = 10 %
  - Cluster Score: (20 + 30 + (60/6000))/3 = 20

3 Ein Cluster Score über 70 wird als „Überkapazität“ betrachtet.

4 Eine „logische ID“ ist eine 128-Bit-UUID, die ein Element im VMware SD-WAN-Netzwerk eindeutig kennzeichnet.

- Beispiel: Jeder Edge wird durch eine logische ID repräsentiert, und jeder Cluster wird durch eine logische ID repräsentiert.
- Während der Benutzer die Edge- und die Clusternamen bereitstellt, sind die logischen IDs garantiert eindeutig und werden für die interne Identifizierung der Elemente verwendet.

Wie werden SD-WAN Edge-Cluster vom SD-WAN Gateway verfolgt?

Sobald ein Hub zu einem VMware SD-WAN-Cluster hinzugefügt wird, bricht der Hub ab und erstellt die Tunnel zu allen ihm zugewiesenen Gateways neu. Außerdem wird jedem Gateway angezeigt, dass der Hub einem Cluster zugewiesen wurde, und eine logische Cluster-ID wird angegeben.

Für den Cluster verfolgt das SD-WAN Gateway Folgendes:

- Die logische ID
- Den Namen
- Ob die automatische Neuverteilung aktiviert ist
- Eine Liste mit Hub-Objekten für Mitglieder des Clusters

Für jedes Hub-Objekt im Cluster verfolgt das Gateway Folgendes:

- Die logische ID
- Den Namen
- Eine Reihe von Statistiken, die alle 30 Sekunden durch eine periodische Nachricht aktualisiert werden, die vom Hub an jedes zugewiesene Gateway gesendet wird, einschließlich:
  - Aktuelle CPU-Nutzung des Hubs
  - Aktuelle Arbeitsspeichernutzung des Hubs
  - Aktuelle Tunnelzahl auf dem Hub

    - Aktuelle Anzahl der BGP-Routen auf dem Hub
- Der aktuelle berechnete Cluster Score basierend auf der oben angegebenen Formel.

Ein Hub wird aus der Liste der Hub-Objekte entfernt, wenn das Gateway mehr als sieben Sekunden lang keine Pakete vom Hub-Edge empfangen hat.

Wie werden SD-WAN Edges einem bestimmten Hub in einem Cluster zugewiesen?

In einer herkömmlichen Hub- und Spoke-Topologie stellt SD-WAN Orchestrator den Edge mit der logischen ID des Hubs zur Verfügung, mit dem er verbunden werden muss. Der Edge fordert bei seinen zugewiesenen Gateways Konnektivitätsinformationen für die logische ID dieses Hubs an, d. h. IP-Adressen und Ports, die der Edge für die Verbindung mit diesem Hub verwendet.

Aus der Perspektive des Edge ist dieses Verhalten identisch mit dem Verhalten beim Verbinden mit einem Cluster. Der Orchestrator teilt dem Edge mit, dass die logische ID des Hubs, mit dem er eine Verbindung herstellen soll, die logische ID des Clusters und nicht die logische ID des einzelnen Hubs ist. Der Edge führt dasselbe Verfahren durch, um eine Hub-Verbindungsanfrage an die Gateways zu senden, und erwartet als Reaktion darauf Verbindungsinformationen.

An diesem Punkt gibt es zwei Abweichungen vom grundlegenden Hub-Verhalten:

- **Abweichung Nr. 1**: Das Gateway muss auswählen, welcher Hub zugewiesen werden soll.
- **Abweichung Nr. 2**: Aufgrund von Abweichung Nr. 1 erhält der Edge möglicherweise verschiedene Zuweisungen von seinen verschiedenen Gateways.

Die Abweichung Nr. 1 wurde ursprünglich angesprochen, indem der Cluster Score verwendet wurde, um den am wenigsten belasteten Hub in einem Cluster einem Edge zuzuweisen. Obwohl dies logisch ist, erwies es sich in der realen Welt als eine nicht ideale Lösung, da ein typisches Neuzuweisungsereignis Hunderte oder sogar Tausende von Edges betreffen kann und der Cluster Score nur alle 30 Sekunden aktualisiert wird. Mit anderen Worten: Wenn Hub 1 einen Cluster Score von 20 und Hub 2 einen Cluster Score von 21 hat, würden alle Edges 30 Sekunden lang Hub 1 wählen, woraufhin dieser überlastet sein und weitere Neuzuweisungen auslösen könnte.

Stattdessen versucht das Gateway zunächst eine faire mathematische Verteilung unter Missachtung des Cluster Score. Die logischen Edge-IDs, die von einem sicheren Zufallszahlengenerator auf dem Orchestrator erzeugt wurden, werden (bei genügend Edges) eine gleichmäßige Verteilung der Werte aufweisen. Das bedeutet, dass anhand der logischen ID eine faire Anteilsverteilung berechnet werden kann.

- Logische Edge-ID **modulo** die Anzahl der Hubs im Cluster = Zugewiesener Hub-Index
- Beispiel:
    - Vier Edges mit logischen IDs, die auf 1, 2, 3, 4 enden
    - Cluster mit 2 Hubs
    - 1 % 2 = 1, 2 % 2 = 0, 3 % 2 = 1, 4 % 2 = 0 (Hinweis: „%“ steht für den Operator „modulo“)
    - Edge 2 und 4 wird der Hub-Index 0 zugewiesen

- Edge 1 und 3 wird der Hub-Index 1 zugewiesen

Diese Vorgehensweise ist konsistenter als eine Zuweisung vom Typ „Round-Robin“, weil es bedeutet, dass den Edges jedes Mal derselbe Hub zugewiesen wird. Dadurch wird die Zuweisung und Fehlerbehebung prädiktiver.

Hinweis Wenn ein Hub neu gestartet wird (z. B. aufgrund von Wartung oder Ausfall), wird er vom Gateway getrennt und aus dem Cluster entfernt. Dies bedeutet, dass die Edges nach dem Neustart aller Edges (aufgrund der oben beschriebenen Logik) immer gleichmäßig verteilt werden, aber nach jedem Hub-Ereignis, das zum Verlust der Konnektivität führt, ungleichmäßig verteilt sind.

Was geschieht, wenn die maximal zulässige Tunnelkapazität eines Hubs überschritten wird?

Die Edge-Zuweisungslogik versucht, die Edges gleichmäßig auf alle verfügbaren Hubs zu verteilen. Nach einem Ereignis (z. B. Neustart) auf dem Hub sind die Edges jedoch nicht mehr gleichmäßig verteilt.

Hinweis In der Regel versucht das Gateway bei der anfänglichen Zuweisung, die Edges gleichmäßig auf Hubs zu verteilen. Eine ungleichmäßige Verteilung wird nicht als ungültiger Zustand betrachtet. Wenn die Zuweisungen ungleichmäßig sind, aber kein einzelner Hub 70 % der Tunnelkapazität überschreitet, gilt die Zuweisung als gültig.

Aufgrund eines solchen Ereignisses auf dem Hub (oder dem Hinzufügen zusätzlicher Edges zum Netzwerk) können Cluster einen Punkt erreichen, an dem ein einzelner Hub 70 % seiner zulässigen Tunnelkapazität überschritten hat. Wenn dies geschieht und mindestens ein weiterer Hub eine Tunnelkapazität von weniger als 70 % aufweist, wird automatisch eine gleichmäßige erneute Verteilung durchgeführt, unabhängig davon, ob die Neuverteilung im Orchestrator aktiviert ist. Die meisten Edges behalten Ihre vorhandene Zuweisung aufgrund der prädiktiven mathematischen Zuweisung mithilfe von logischen IDs bei, und die Edges, die anderen Hubs aufgrund von Failover oder vorheriger Neuverteilung der Nutzung zugewiesen wurden, werden neu verteilt, um sicherzustellen, dass der Cluster automatisch zu einer gleichmäßigen Verteilung zurückkehrt.

Was geschieht, wenn der maximal zulässige Cluster Score eines Hubs überschritten wird?

Im Gegensatz zum Tunnelprozentsatz (ein direktes Maß für die Kapazität), auf den sofort reagiert werden kann, wird der Cluster Score nur alle 30 Sekunden aktualisiert, und das Gateway kann nicht automatisch berechnen, wie hoch der angepasste Cluster Score nach einer Edge-Neuzuweisung sein wird. In der Clusterkonfiguration wird ein Parameter für die automatische Neuverteilung bereitgestellt, um anzugeben, ob das Gateway dynamisch versuchen soll, die Edge-Last für jeden Hub nach Bedarf zu verschieben.

Wenn die automatische Neuverteilung deaktiviert ist und ein Hub einen Cluster Score über 70 hat (aber keine 70 % Tunnelkapazität), wird keine Maßnahme ergriffen.

Wenn die automatische Neuverteilung aktiviert ist und mindestens ein Hub einen Cluster Score von mehr als 70 hat, weist das Gateway dem Hub mit dem niedrigsten Cluster Score einen Edge pro Minute zu, bis alle Hubs unter 70 liegen oder keine Neuzuweisungen mehr möglich sind.

Hinweis Die automatische Neuverteilung ist standardmäßig deaktiviert.

Was geschieht, wenn zwei SD-WAN-Gateways unterschiedliche Hub-Zuweisungen vornehmen?

Wie es der Natur einer verteilten Steuerungsebene entspricht, bestimmt jedes Gateway die Clusterzuweisung individuell. In den meisten Fällen verwenden Gateways dieselbe mathematische Formel und gelangen somit zur gleichen Zuweisung für alle Edges. In Fällen wie der auf dem Cluster Score basierenden Neuverteilung kann dies jedoch nicht gewährleistet werden.

Wenn ein Edge zurzeit nicht mit einem Hub in einem Cluster verbunden ist, akzeptiert er die Zuweisung von jedem Gateway, das antwortet. Dadurch wird sichergestellt, dass Edges in einem Szenario, in dem einige Gateways ausgefallen sind und andere aktiv sind, nie ohne Zuweisung bleiben.

Wenn ein Edge mit einem Hub in einem Cluster verbunden ist und eine Nachricht erhält, die angibt, dass er einen alternativen Hub wählen soll, wird diese Nachricht in der Reihenfolge der „Gateway-Präferenz“ verarbeitet. Ist beispielsweise das Super-Gateway verbunden, akzeptiert der Edge nur Neuzuweisungen vom Super-Gateway. In Konflikt stehende Zuweisungen, die von anderen Gateways angefordert werden, werden ignoriert. Ebenso würde der Edge, wenn das Super-Gateway nicht angeschlossen ist, nur Neuzuweisungen vom alternativen Super-Gateway akzeptieren. Für Partner-Gateways (wenn keine Super-Gateways vorhanden sind) basiert die Voreinstellung des Gateways auf der Reihenfolge der konfigurierten Partner-Gateways für diesen spezifischen Edge.

Was geschieht, wenn ein SD-WAN Gateway ausfällt?

Wenn ein SD-WAN Gateway ausfällt, werden die Edges möglicherweise neu zugewiesen, wenn das Gateway mit der höchsten Priorität dasjenige ist, das ausgefallen ist, und das Gateway mit der nächsthöheren Priorität eine andere Zuweisung bereitgestellt hat. Beispiel: Das Super-Gateway hat Hub A diesem Edge zugewiesen, während das alternative Super-Gateway Hub B demselben Edge zugewiesen hat.

Das Super-Gateway, das ausfällt, löst ein Failover des Edge zu Hub B aus, da das alternative Super-Gateway jetzt das Gateway mit der höchsten Priorität für die Konnektivitätsinformationen ist.

Wenn das-Super-Gateway wiederhergestellt wird, fordert der Edge erneut eine Hub-Zuweisung von diesem Gateway an. Um zu verhindern, dass der Edge im obigen Szenario wieder zu Hub A wechselt, enthält die Hub-Zuweisungsanforderung den zurzeit zugewiesenen Hub (sofern vorhanden). Wenn das Gateway die Zuweisungsanforderung verarbeitet, falls dem Edge zurzeit ein Hub im Cluster zugewiesen ist und dieser Hub einen Cluster Score von weniger als 70 hat,

aktualisiert das Gateway seine lokale Zuweisung, damit sie mit der vorhandenen Zuweisung übereinstimmt, ohne seine Zuweisungslogik zu durchlaufen. Auf diese Weise wird sichergestellt, dass das Super-Gateway bei Wiederherstellung den aktuell verbundenen Hub zuweist und ein unnötiges Failover für seine zugewiesenen Edges verhindert.

Was geschieht, wenn ein Hub in einem Cluster seine dynamischen Routen verliert?

Die Hubs melden den SD-WAN Gateways alle 30 Sekunden die Anzahl der dynamischen Routen, die sie über BGP gelernt haben. Wenn Routen für nur einen Knoten in einem Cluster verloren gehen, weil sie fälschlicherweise zurückgezogen werden oder die BGP-Nachbarschaft ausfällt, führen die SD-WAN Gateways ein Failover der Spoke Edges auf einen anderen Hub in dem Cluster durch, der eine intakte Routing-Tabelle aufweist.

Da die Updates alle 30 Sekunden gesendet werden, basiert die Routenanzahl auf dem Zeitpunkt, an dem das Update an das SD-WAN-Gateway gesendet wird. Die Neuverteilungslogik für das SD-WAN-Gateway wird alle 60 Sekunden ausgeführt. Das bedeutet, dass Benutzer im unwahrscheinlichen Fall eines Totalausfalls eines LAN-seitigen BGP-Nachbarn mit einem Failover von 30 – 60 Sekunden rechnen können. Um sicherzustellen, dass alle Hubs nach einem solchen Ereignis die Möglichkeit haben, die SD-WAN-Gateways erneut zu aktualisieren, ist die Neuverteilung auf maximal einmal pro 120 Sekunden begrenzt. Dies bedeutet, dass die Benutzer bei einem zweiten aufeinander folgenden Ausfall mit einem Failover von 120 Sekunden rechnen können.

Was passiert, wenn ein Hub in einem Cluster ausfällt?

Das SD-WAN Gateway wartet 7 Sekunden lang darauf, dass die Tunnel für inaktiv erklärt werden, bevor ein Failover zu Spoke Edges durchgeführt wird. Das bedeutet, dass Benutzer mit einem Failover von 7 – 10 Sekunden (abhängig von RTT) rechnen können, wenn ein SD-WAN-Hub oder alle zugehörigen WAN-Links ausfallen.

Konfigurieren von Edge-Clustering

Sie können Edge-Cluster konfigurieren, indem Sie die Schritte in diesem Abschnitt ausführen.

1 Navigieren Sie für den Zugriff auf den Bereich **Edge-Cluster (Edge Cluster)** zu **Konfigurieren (Configure) > Netzwerkdienste (Network Services)**.

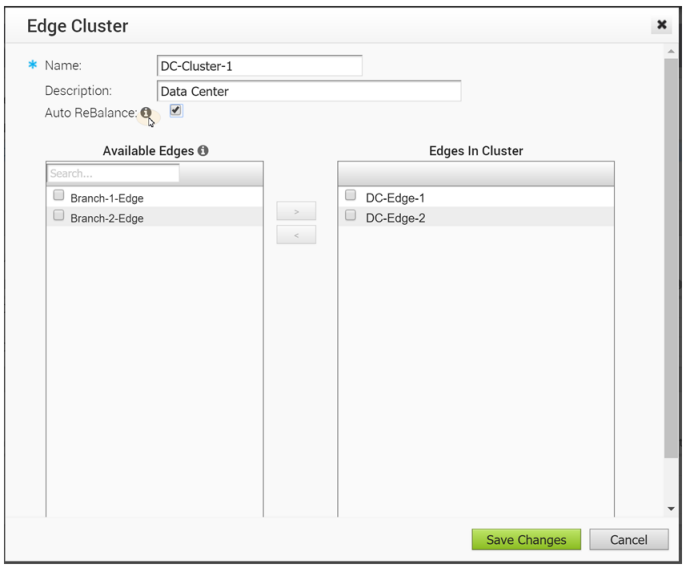
2 So fügen Sie einen neuen Cluster hinzu:

   a Klicken Sie im Bereich **Edge-Cluster (Edge Cluster)** auf die Schaltfläche **Neuer Cluster (New Cluster)**.

   b Geben Sie im Dialogfeld **Edge-Cluster (Edge Cluster)** den Text und die Beschreibung in den entsprechenden Textfeldern ein.

c Aktivieren Sie gegebenenfalls **Automatische Neuverteilung (Auto Rebalance)** (diese Funktion ist standardmäßig nicht aktiviert).

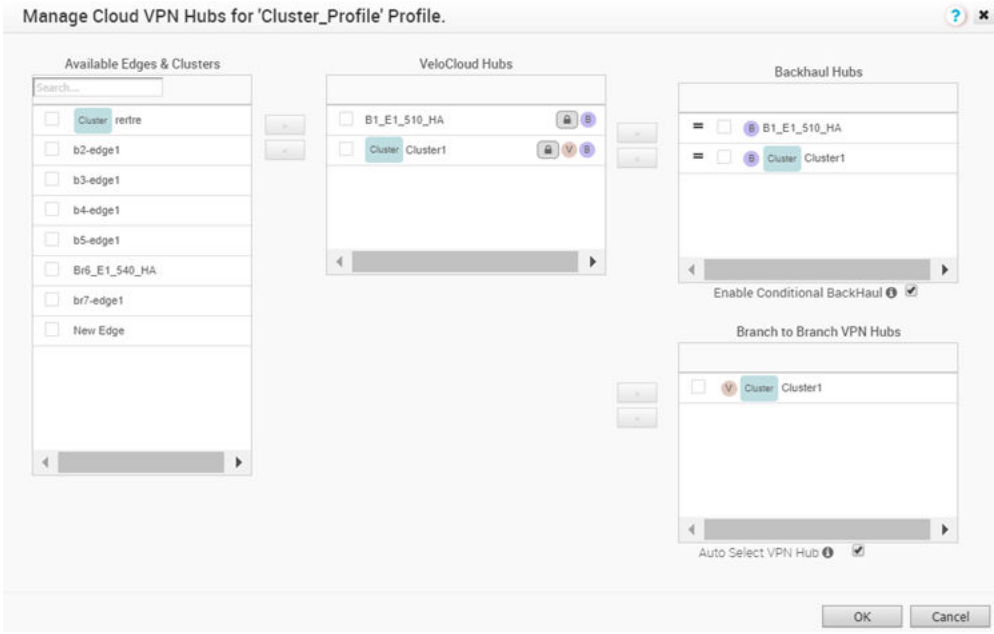
Hinweis Folgende Erläuterung wird in der QuickInfo zu „Automatische Neuverteilung (Auto Rebalance)“ im VMware SD-WAN Orchestrator bereitgestellt: Wenn bei aktivierter Option ein einzelner Edge in einem Hub-Cluster den Cluster Score von 70 überschreitet, werden Spokes mit einer Rate von einem Spoke pro Minute neu verteilt, bis der Cluster Score auf unter 70 sinkt. Wenn ein Spoke-Edge einem anderen Hub zugewiesen wird, werden die VPN-Tunnel des Spoke-Edge getrennt und es kommt unter Umständen zu einer Ausfallzeit von bis zu 6 bis 10 Sekunden. Wenn alle Hubs in einem Cluster den Cluster Score von 70 überschreiten, wird keine Neuverteilung durchgeführt. Weitere Informationen zum Cluster Score finden Sie im Abschnitt Funktionsweise von Edge-Clustering.



d Wählen Sie im Abschnitt **Verfügbare Edges (Available Edges)** einen Edge aus und verschieben Sie ihn in den Abschnitt **Edges im Cluster (Edges In Cluster)**, indem Sie die Schaltfläche **>** verwenden.

e Klicken Sie auf **Änderungen speichern (Save Changes)**. Der konfigurierte Edge-Cluster wird im Bereich **Verfügbare Edges und Cluster (Available Edges & Clusters)** des Bildschirms **Cloud-VPN-Hubs verwalten (Manage Cloud VPN Hubs)** für das ausgewählte Profil angezeigt.

Hinweis Edges, die als Hub oder in Hub-Clustern verwendet werden oder als Aktiv/Standby-HA-Paar konfiguriert sind, werden nicht im Listenbereich **Verfügbare Edges (Available Edges)** angezeigt.



3 Über den Bildschirm **Cloud-VPN-Hubs verwalten (Manage Cloud VPN Hubs)** können Sie einen Edge-Cluster und einen einzelnen Edge gleichzeitig als Hubs in einem Zweigstellenprofil konfigurieren. Sobald Edges einem Cluster zugewiesen sind, können sie nicht mehr als einzelne Hubs zugewiesen werden. Wählen Sie einen Edge-Cluster als Hub im Zweigstellenprofil aus.

4 Zum Konfigurieren eines Zweigstelle-zu-Zweigstelle-VPN mithilfe von Hubs, die auch als Edge-Cluster fungieren, wählen Sie zuerst einen Hub im Bereich **VeloCloud-Hubs (VeloCloud Hubs)** aus und verschieben ihn in den Bereich **Zweigstelle-zu-Zweigstelle-VPN-Hubs (Branch to Branch VPN Hubs)**.

5 Hub-Cluster können auch als Internet-Backhaul-Hubs in der Unternehmensrichtlinienkonfiguration konfiguriert werden, indem Sie zuerst einen Hub im Bereich **VeloCloud-Hubs (VeloCloud Hubs)** auswählen und ihn dann in den Bereich **Backhaul-Hubs (Backhaul Hubs)** verschieben.

6 Zum Aktivieren von bedingtem Backhaul aktivieren Sie das Kontrollkästchen **Bedingtes Backhaul aktivieren (Enable Conditional BackHaul**). Wenn der bedingte Backhaul (CBH) aktiviert ist, kann der Edge ein Failover von internetgebundenem Datenverkehr (direkter Internetdatenverkehr, Internet über SD-WAN Gateway und Datenverkehr für Cloud-Sicherheit über IPsec) zu MPLS-Verbindungen durchführen, wenn keine öffentlichen Internetverbindungen verfügbar sind. Wenn die Funktion „Bedingter Backhaul“ aktiviert ist, unterliegen standardmäßig alle Unternehmensrichtlinienregeln auf der Zweigstellenebene dem Failover des Datenverkehrs über bedingten Backhaul. Sie können den Datenverkehr vom bedingten Backhaul basierend auf bestimmten Anforderungen für ausgewählte Richtlinien ausschließen, indem Sie diese Funktionen auf der ausgewählten Unternehmensrichtlinienebene deaktivieren. Weitere Informationen finden Sie unter Bedingter Backhaul.

Fehlerbehebung bei Edge-Clustering

In diesem Abschnitt werden die Verbesserungen bei der Fehlerbehebung für Edge-Clustering beschrieben.

Übersicht

Das Edge-Clustering umfasst eine Fehlerbehebungsfunktion, mit der SD-WAN-Spoke-Edges von VMware in einem Cluster neu verteilt werden können. Die Neuverteilung der Spokes kann auf jedem der Hubs im Cluster durchgeführt werden. Es gibt zwei Methoden für die Neuverteilung von Spokes:

- Gleichmäßige Neuverteilung von Spokes auf alle Hubs im Cluster.
- Ausschließen eines Hubs und Neuverteilung der Spokes auf die verbleibenden Hubs im Cluster.

Neuverteilung von Spokes auf dem Hub mithilfe von VMware SD-WAN Orchestrator

Ein Administrator kann die Spokes in einem Cluster über die Option **Remote-Diagnose (Remote Diagnostics)** in SD-WAN Orchestrator neu verteilen. Wenn ein VMware SD-WAN Edge als Hub in einem Cluster bereitgestellt wird, wird eine neue Remote-Diagnoseoption namens **Hub-Cluster neu verteilen (Rebalance Hub Cluster)** angezeigt, die Benutzern zwei Möglichkeiten bietet.

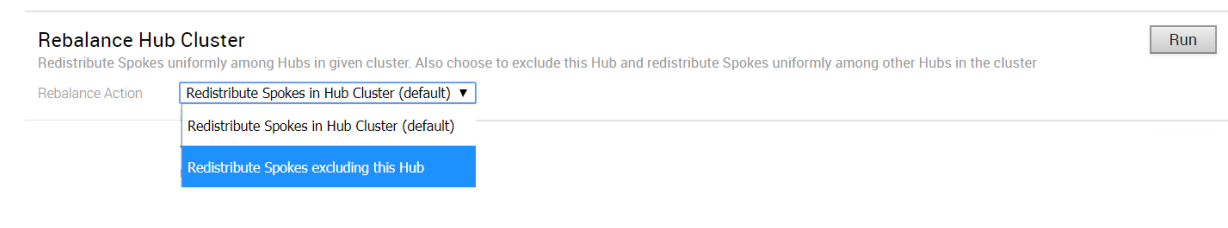
Neuverteilung von Spokes im Hub-Cluster (Redistribute Spokes in Hub Cluster)

- Mit dieser Option wird versucht, die Spoke-Edges gleichmäßig auf alle Hub-Edges im Cluster neu zu verteilen.

Neuverteilung von Spokes mit Ausnahme dieses Hubs (Redistribute Spokes excluding this Hub)

- Mit dieser Option wird versucht, die Spokes gleichmäßig auf die Hubs im Cluster neu zu verteilen. Dabei wird der Hub-Edge, von dem aus ein Benutzer das Dienstprogramm für die Neuverteilung von Spokes ausführt, ausgeschlossen.
- Diese Option kann für die Fehlerbehebung oder Wartung verwendet werden, um alle Spokes von diesem Hub-Edge zu entfernen.

Nachfolgend finden Sie eine Abbildung des Abschnitts **Remote-Diagnose (Remote Diagnostics)** des Hubs.



Hinweis Die Neuverteilung der Spokes führt zu einer kurzen Unterbrechung des Datenverkehrs, wenn der Spoke auf einen anderen Hub im Cluster verschoben wird. Aus diesem Grund wird dringend empfohlen, dieses Verfahren zur Fehlerbehebung während eines Wartungsfensters zu verwenden.

Konfigurieren einer Non VMware SD-WAN Site

VMware SD-WAN unterstützt die folgenden Non VMware SD-WAN Site-Konfigurationen:

- Check Point
- Cisco ASA
- Cisco ISR
- Generischer IKEv2-Router (routenbasiertes VPN)
- Microsoft Azure Virtual Hub
- Palo Alto
- SonicWALL
- Zscaler
- Generischer IKEv1-Router (routenbasiertes VPN)
- Generische Firewall (richtlinienbasiertes VPN)

Hinweis VMware SD-WAN unterstützt jetzt Non VMware SD-WAN Site-Konfigurationen mit dem generischen IKEv1-Router (routenbasiertes VPN) und mit dem generischen IKEv2-Router (routenbasiertes VPN).

Cisco ASA

Cisco ASA ist eine weitere gängige Drittanbieterkonfiguration. Anweisungen zur Konfiguration mit Cisco ASA im SD-WAN Orchestrator werden unten aufgelistet.

So führen Sie eine Konfiguration über Cisco ASA durch:

1 Navigieren Sie zu **Konfigurieren (Configure) > Netzwerkdienste (Network Services)**.

2 Klicken Sie im Bereich **Nicht-VeloCloud-Sites (Non-VeloCloud Sites)** auf die Schaltfläche **Neu (New)**.

Das Dialogfeld **Neue Nicht-VeloCloud-Site (New Non-VeloCloud Site)** wird angezeigt.

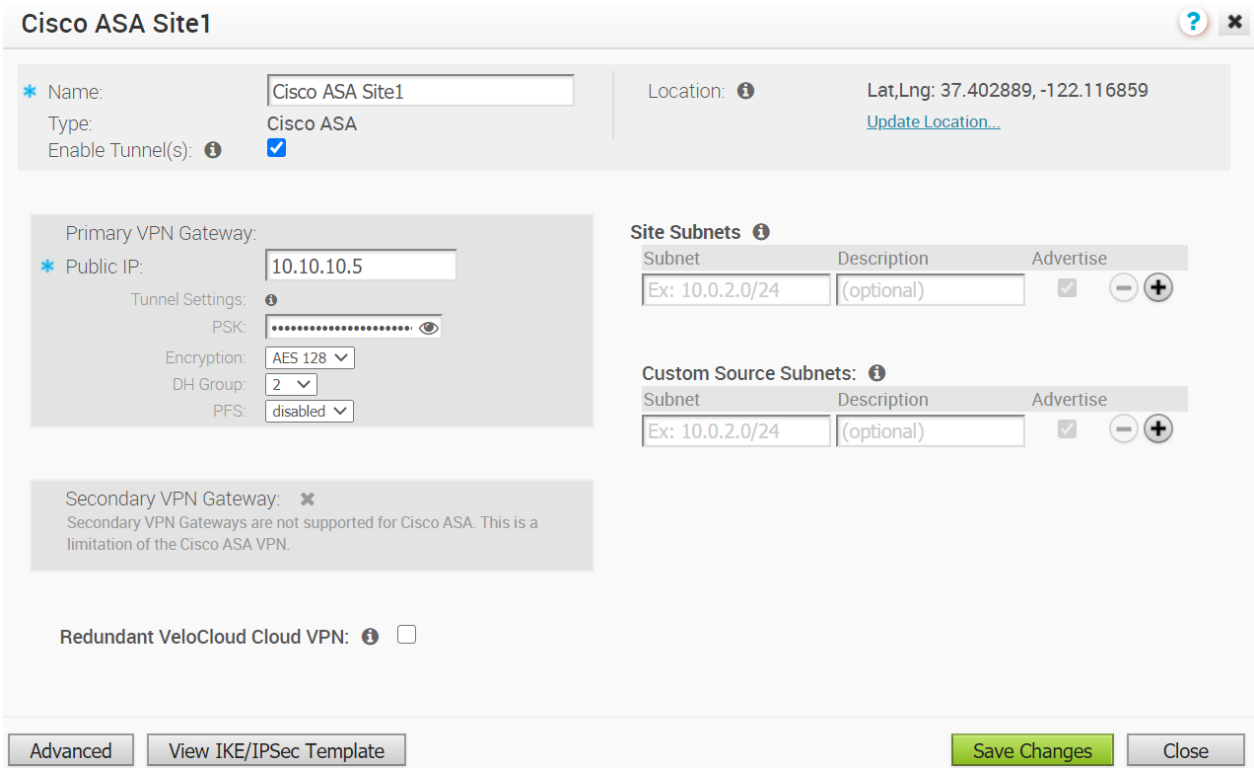
3 Gehen Sie im Dialogfeld **Neue Nicht-VeloCloud-Site (New Non-VeloCloud Site)** wie folgt vor:

a Geben Sie im Textfeld **Name** den Namen für die Non VMware SD-WAN Site ein.

b Wählen Sie im Dropdown-Menü **Typ (Type)** den Eintrag **Cisco ASA** aus.

c Geben Sie die IP-Adresse für das primäre VPN-Gateway ein und klicken Sie auf **Weiter (Next)**.

Ihre Non VMware SD-WAN Site wird erstellt, und ein Dialogfeld für Ihre Non VMware SD-WAN Site wird angezeigt.



4 Gehen Sie im Dialogfeld für Ihre Non VMware SD-WAN Site wie folgt vor:

a Um Tunneleinstellungen für das primäre VPN-Gateway der Non VMware SD-WAN Site zu konfigurieren, klicken Sie auf die Schaltfläche **Erweitert (Advanced)**, die sich am unteren Rand des Dialogfelds befindet.

b Im Bereich **Primäres VPN-Gateway (Primary VPN Gateway)** können Sie die folgenden Tunneleinstellungen konfigurieren:

Feld	Beschreibung
PSK	Der vorinstallierte Schlüssel (Pre-Shared Key, PSK), der der Sicherheitsschlüssel für die Authentifizierung über den Tunnel ist. Der Orchestrator generiert standardmäßig einen PSK. Wenn Sie einen eigenen PSK oder ein eigenes Kennwort verwenden möchten, können Sie dies in das Textfeld eingeben.
Verschlüsselung (Encryption)	Wählen Sie entweder **AES 128** oder **AES 256** als Algorithmus zum Verschlüsseln von Daten aus. Der Standardwert ist AES 128.
DH-Gruppe (DH Group)	Wählen Sie den Diffie-Hellman (DH)-Gruppen-Algorithmus aus, der beim Austausch eines vorinstallierten Schlüssels verwendet werden soll. Über die DH-Gruppe wird die Stärke des Algorithmus in Bit festgelegt. Der Standardwert ist 2.
PFS	Wählen Sie die PFS-Ebene (Perfect Forward Secrecy) für zusätzliche Sicherheit aus. Der Standardwert ist 2.

Hinweis Das sekundäre VPN-Gateway wird für den Netzwerkdiensttyp Cisco ASA nicht unterstützt.

Hinweis Bei einer Non VMware SD-WAN Site vom Typ Cisco ASA ist der standardmäßig verwendete lokale Authentifizierungs-ID-Wert die lokale IP der SD-WAN Gateway-Schnittstelle.

c Aktivieren Sie das Kontrollkästchen **Redundantes VeloCloud-Cloud-VPN (Redundant VeloCloud Cloud VPN)**, um redundante Tunnel für jedes VPN-Gateway hinzuzufügen.

Alle Änderungen, die an „Verschlüsselung (Encryption)“, „DH-Gruppe (DH Group)“ oder „PFS von Primäres VPN-Gateway (PFS of Primary VPN Gateway)“ vorgenommen wurden, werden, falls konfiguriert, auch auf die redundanten VPN-Tunnel angewendet. Nachdem Sie die Tunneleinstellungen des primären VPN-Gateways geändert haben, speichern Sie die Änderungen und klicken dann auf **IKE/IPSec-Vorlage anzeigen (View IKE/IPSec Template)**, um die aktualisierte Tunnelkonfiguration anzuzeigen.

d Klicken Sie auf den Link **Standort aktualisieren (Update location)**, um den Standort für die konfigurierte Non VMware SD-WAN Site anzuzeigen. Die Angaben zum Längen- und Breitengrad werden verwendet, um den besten Edge oder das beste Gateway zu bestimmen, mit dem eine Verbindung im Netzwerk hergestellt werden kann.

e Unter **Site-Subnetze (Site Subnets)** können Sie Subnetze für die Non VMware SD-WAN Site hinzufügen, indem Sie auf die Schaltfläche mit dem Pluszeichen (**+**) klicken.

f Verwenden Sie **Benutzerdefinierte Quellsubnetze (Custom Source Subnets)**, um die an dieses VPN-Gerät weitergeleiteten Quellsubnetze außer Kraft zu setzen. Normalerweise werden Quellsubnetze von den an dieses Gerät weitergeleiteten Edge-LAN-Subnetzen abgeleitet.

g Aktivieren Sie das Kontrollkästchen **Tunnel aktivieren (Enable Tunnel(s))**, sobald Sie bereit sind, den Tunnel vom SD-WAN Gateway zu den Cisco ASA-VPN-Gateways zu initiieren.

h Klicken Sie auf **Änderungen speichern (Save Changes)**.

Cisco ISR

Cisco ISR ist eine der gängigeren Drittanbieterkonfigurationen. Anweisungen zur Konfiguration mit Cisco ISR in SD-WAN Orchestrator sind unten aufgelistet.

So führen Sie eine Konfiguration über Cisco ISR durch:

1 Navigieren Sie zu **Konfigurieren (Configure) > Netzwerkdienste (Network Services)**.

2 Klicken Sie im Bereich **Nicht-VeloCloud-Sites (Non-VeloCloud Sites)** auf die Schaltfläche **Neu (New)**.

Das Dialogfeld „Neue Nicht-VeloCloud-Site“ (New Non-VeloCloud Site) wird angezeigt.

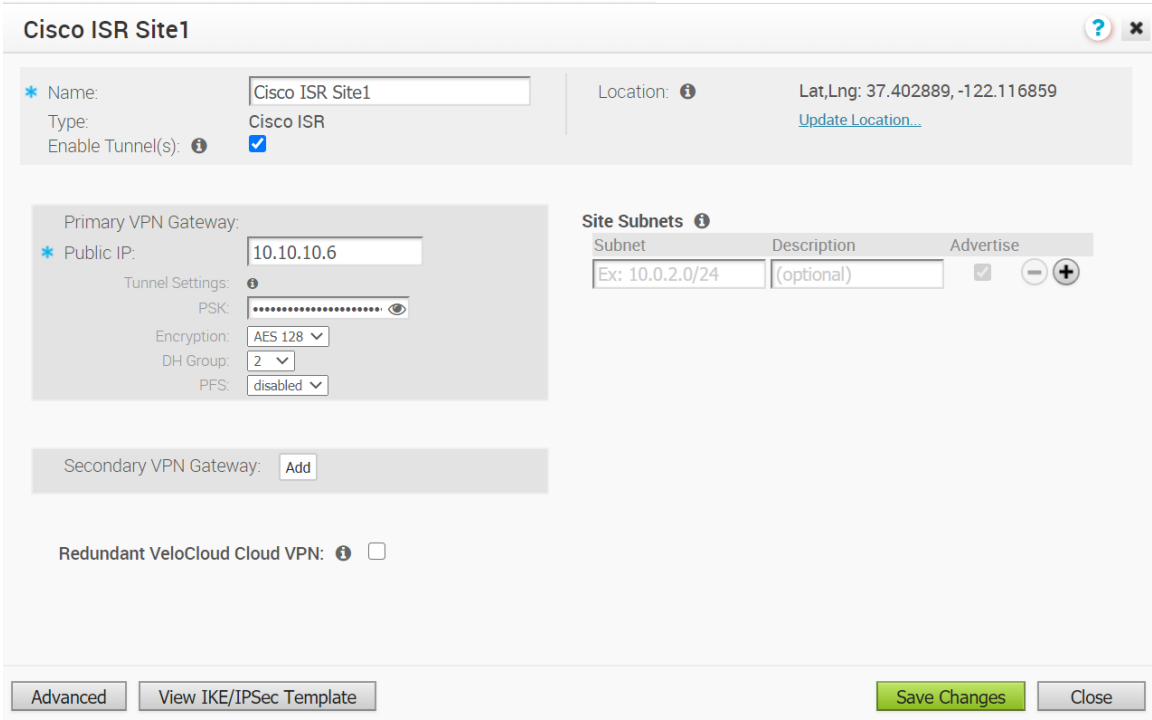
3 Gehen Sie im Dialogfeld **Neue Nicht-VeloCloud-Site (New Non-VeloCloud Site)** wie folgt vor:

a Geben Sie im Textfeld **Name** den Namen für die Non VMware SD-WAN Site ein.

b Wählen Sie im Dropdown-Menü **Typ (Type)** den Eintrag **Cisco ISR** aus.

c Geben Sie die IP-Adresse für das primäre VPN-Gateway ein und klicken Sie auf **Weiter (Next)**.

Ihre Non VMware SD-WAN Site wird erstellt, und ein Dialogfeld für Ihre Non VMware SD-WAN Site wird angezeigt.



4 Gehen Sie im Dialogfeld für Ihre Non VMware SD-WAN Site wie folgt vor:

a Um Tunneleinstellungen für das primäre VPN-Gateway der Non VMware SD-WAN Site zu konfigurieren, klicken Sie auf die Schaltfläche **Erweitert (Advanced)**, die sich am unteren Rand des Dialogfelds befindet.

b Konfigurieren Sie Tunneleinstellungen, wie z. B. PSK, Verschlüsselung (Encryption), DH-Gruppe (DH Group) und PFS, unter Beachtung der obigen Tabelle.

c Wenn Sie ein sekundäres VPN-Gateway für diese Site erstellen möchten, klicken Sie auf die Schaltfläche **Hinzufügen (Add)** neben **Sekundäres VPN-Gateway (Secondary VPN Gateway)**. Geben Sie im Popup-Fenster die IP-Adresse des sekundären VPN-Gateways ein und klicken Sie auf **Änderungen speichern (Save Changes)**.

Das sekundäre VPN-Gateway wird sofort für diese Site erstellt und stellt einen VMware SD-WAN-VPN-Tunnel für dieses Gateway bereit.

Hinweis Bei einer Non VMware SD-WAN Site vom Typ Cisco ISR ist der standardmäßig verwendete lokale Authentifizierungs-ID-Wert die lokale IP der SD-WAN Gateway-Schnittstelle.

d Aktivieren Sie das Kontrollkästchen **Redundantes VeloCloud-Cloud-VPN (Redundant VeloCloud Cloud VPN)**, um redundante Tunnel für jedes VPN-Gateway hinzuzufügen.

e Unter **Site-Subnetze (Site Subnets)** können Sie Subnetze für die Non VMware SD-WAN Site hinzufügen, indem Sie auf die Schaltfläche mit dem Pluszeichen (**+**) klicken.

f Aktivieren Sie das Kontrollkästchen **Tunnel aktivieren (Enable Tunnel(s))**, sobald Sie bereit sind, den Tunnel vom SD-WAN Gateway zu den Cisco ISR-VPN-Gateways zu initiieren.

g Klicken Sie auf **Änderungen speichern (Save Changes)**.

Microsoft Azure Virtual Hub

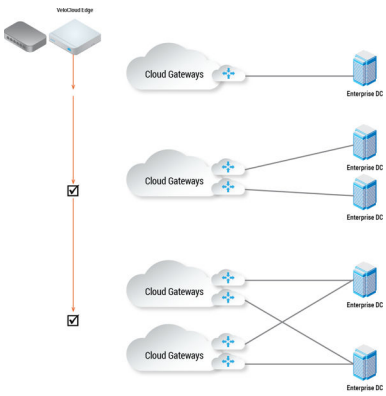
Microsoft Azure Virtual Hub ist eine der gängigeren Drittanbieterkonfigurationen. Anweisungen zum Konfigurieren einer Non VMware SD-WAN Site vom Typ Microsoft Azure Virtual Hub in SD-WAN Orchestrator finden Sie unter Konfigurieren einer Microsoft Azure-Non VMware SD-WAN Site.

VPN-Workflow

Dies ist ein optionaler Dienst, mit dem Sie VPN-Tunnelkonfigurationen für den Zugriff auf mindestens eine Non VMware SD-WAN Sites erstellen können. Das VMware SD-WAN stellt die Konfiguration bereit, die zum Erstellen der Tunnel erforderlich sind, einschließlich der Erstellung einer IKE-IPSec-Konfiguration und der Erzeugung eines vorinstallierten Schlüssels.

Übersicht

Die folgende Abbildung zeigt einen Überblick über die VPN-Tunnel, die zwischen VMware SD-WAN und einer Non VMware SD-WAN Site erstellt werden können.

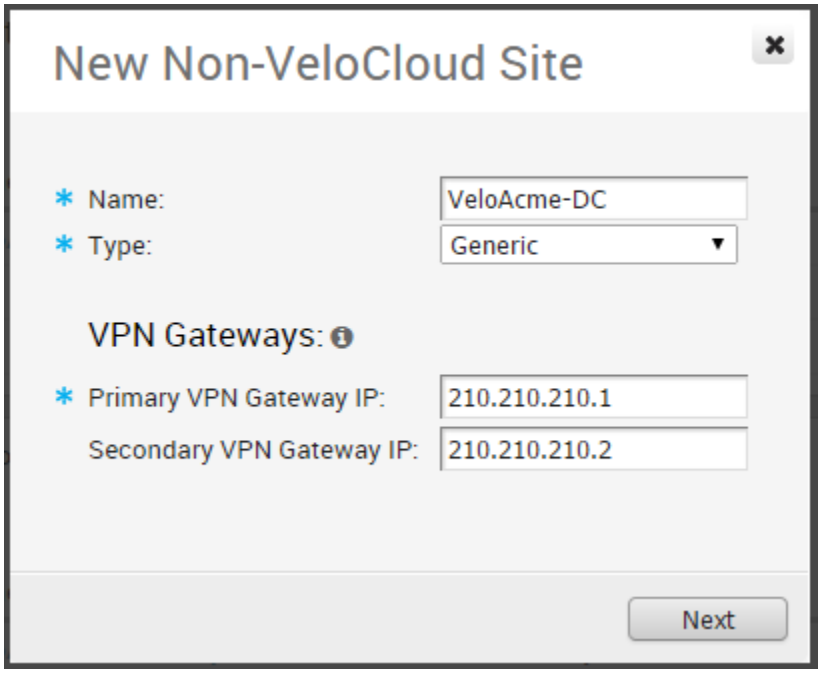


Hinweis Für ein primäres VPN-Gateway auf der Non VMware SD-WAN Site muss eine IP-Adresse angegeben werden. Die IP-Adresse wird verwendet, um einen primären VPN-Tunnel zwischen einem SD-WAN Gateway und dem primären VPN-Gateway zu bilden.

Optional kann eine IP-Adresse für ein sekundäres VPN-Gateway angegeben werden, um einen sekundären VPN-Tunnel zwischen einem SD-WAN Gateway und dem sekundären VPN-Gateway zu bilden. Mithilfe von erweiterten Einstellungen können redundante VPN-Tunnel für alle von Ihnen erstellten VPN-Tunnel angegeben werden.

Hinzufügen eines Non VMware SD-WAN Site-VPN-Gateways

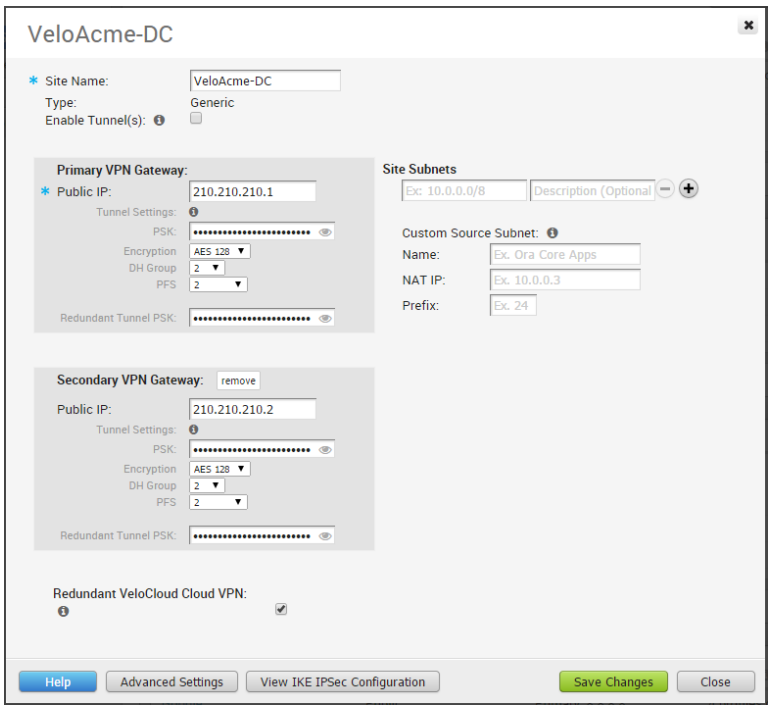
Geben Sie einen Namen ein und wählen Sie einen Gateway-Typ aus. Geben Sie die IP-Adresse für das primäre VPN-Gateway an und geben Sie optional eine IP-Adresse für ein sekundäres VPN-Gateway an.



Konfigurieren von Non VMware SD-WAN Site-Subnetzen

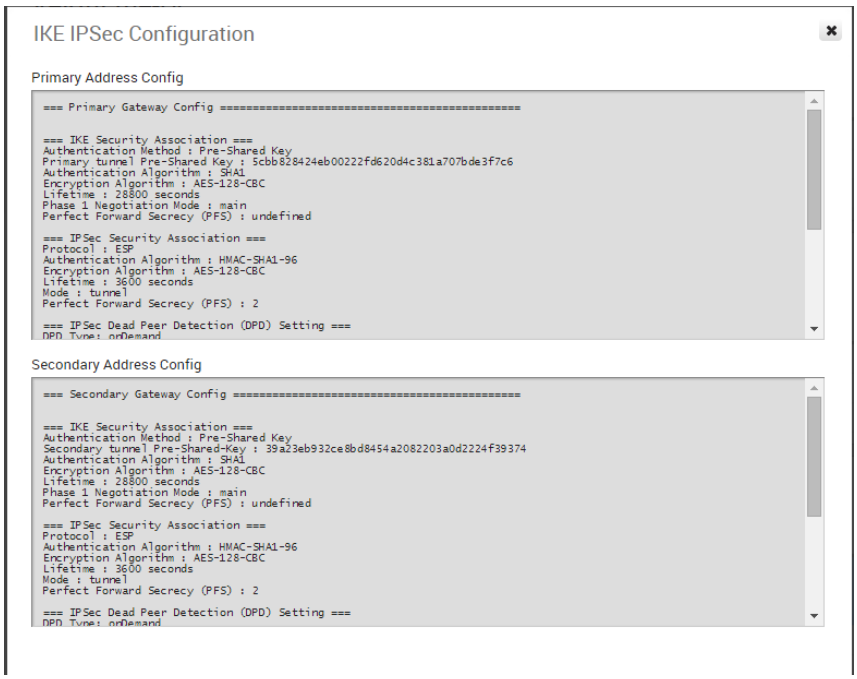
Sobald Sie eine Non VMware SD-WAN Site-Konfiguration erstellt haben, können Sie Site-Subnetze hinzufügen und Tunneleinstellungen konfigurieren.

Klicken Sie auf die Schaltfläche **Erweiterte Einstellungen (Advanced Settings)**, um weitere Subnetzparameter und VPN-Gateway-Parameter einzugeben und redundante VPN-Tunnel hinzuzufügen.



IKE-IPSec-Konfiguration anzeigen, Konfigurieren eines Non VMware SD-WAN Site-Gateways

Wenn Sie auf die Schaltfläche „IKE-IPSec-Konfiguration anzeigen“ (View IKE IPSec Configuration) klicken, werden die Informationen, die zum Konfigurieren des Non VMware SD-WAN Site-Gateways benötigt werden, angezeigt. Der Gateway-Administrator sollte diese Informationen verwenden, um den/die VPN-Tunnel des Gateways zu konfigurieren.



Aktivieren des IPSec-Tunnels

Der Non VMware SD-WAN Site-VPN-Tunnel ist anfangs deaktiviert. Sie müssen den/die Tunnel aktivieren, nachdem das Non VMware SD-WAN Site-Gateway konfiguriert wurde und vor der erstmaligen Verwendung des Edge-zu-Non VMware SD-WAN Site-VPN.

Konfigurieren von Check Point

Das SD-WAN Gateway stellt mithilfe von IKEv1/IPsec eine Verbindung zum Check Point-CloudGuard-Dienst her. Es gibt zwei Schritte, um Check Point zu konfigurieren: Konfigurieren des Check Point-CloudGuard-Diensts und Konfigurieren von Check Point auf der SD-WAN Orchestrator-Instanz. Sie führen den ersten Schritt auf dem Check Point-Infinity-Portal und den zweiten Schritt auf der SD-WAN Orchestrator-Instanz aus.

Klicken Sie auf die Links für die folgenden Abschnitte unten, um die Anweisungen zur Konfiguration von Check Point zu befolgen.

Schritt 1:Konfigurieren von CloudGuard Connect von Check Point

Schritt 2: Konfigurieren von Check Point als Non VMware SD-WAN Site auf SD-WAN Orchestrator

Voraussetzungen

Sie müssen über ein aktives Check Point-Konto und über Anmeldeinformationen verfügen, um auf das Infinity-Portal von Check Point zugreifen zu können.

Konfigurieren von CloudGuard Connect von Check Point

Anweisungen zum Konfigurieren des CloudGuard-Diensts von Check Point.

Sie müssen über ein aktives Check Point-Konto und über Anmeldeinformationen verfügen, um auf das Infinity-Portal von Check Point zugreifen zu können.

Verfahren

1. Um den CloudGuard-Dienst von Check Point zu konfigurieren, melden Sie sich unter https://portal.checkpoint.com/ beim Infinity Portal von Check Point an.
2. Nachdem Sie sich angemeldet haben, erstellen Sie im Infinity Portal von Check Point eine Site über den folgenden Link: https://sc1.checkpoint.com/documents/integrations/VeloCloud/check-point-VeloCloud-integration.html

   Nachdem Sie eine Site im Infinity Portal von Check Point erstellt haben, gehen Sie wie unter Konfigurieren von Check Point als Non VMware SD-WAN Site auf SD-WAN Orchestrator beschrieben vor.

Konfigurieren von Check Point als Non VMware SD-WAN Site auf SD-WAN Orchestrator

Nachdem Sie eine Site im Infinity-Portal von Check Point erstellt haben, konfigurieren Sie Check Point als die Non VMware SD-WAN Site auf der SD-WAN Orchestrator-Instanz.

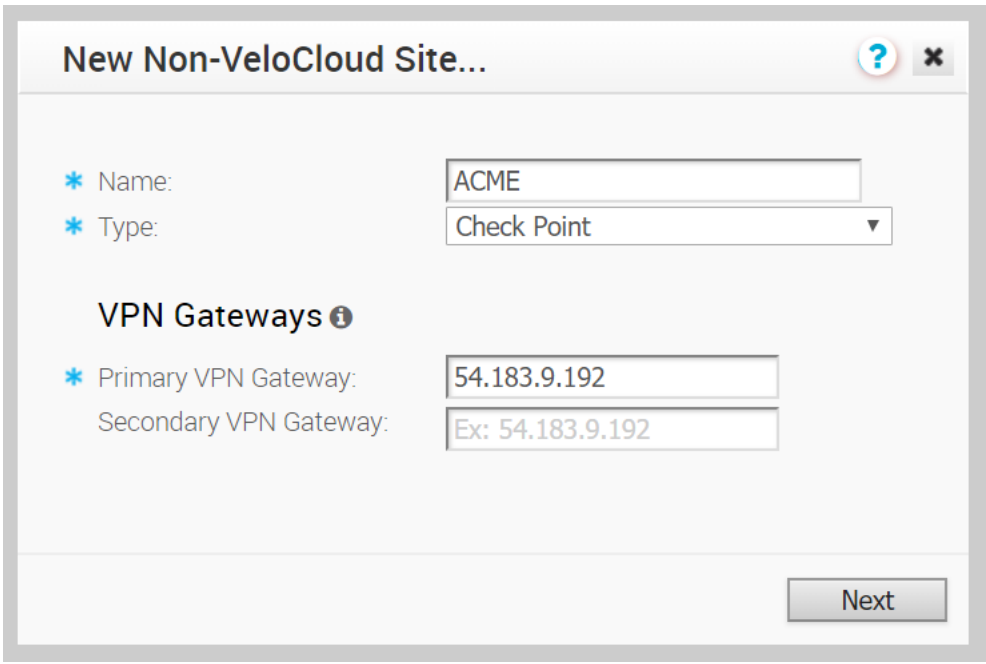
Nachdem Sie eine Site im Infinity-Portal von Check Point erstellt haben, führen Sie die folgenden Schritte aus:

Verfahren

1 Navigieren Sie in SD-WAN Orchestrator zu **Konfigurieren (Configure) > Netzwerkdienste (Network Services)**.

2 Klicken Sie im Bereich **Nicht-VeloCloud-Sites (Non-VeloCloud Sites)** auf die Schaltfläche **Neu (New)**.

Das Dialogfeld **Neue Nicht-VeloCloud-Site (New Non-VeloCloud Site)** wird angezeigt.



3 Führen Sie die folgenden Unterschritte im Dialogfeld **Neue Nicht-VeloCloud-Site (New Non-VeloCloud Site)** aus:

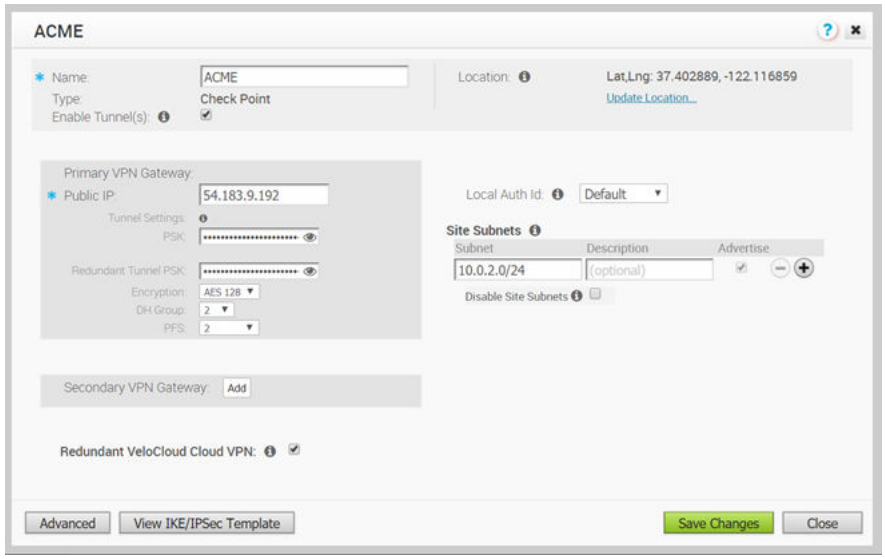
a Geben Sie den Name Ihrer Site ein.

b Wählen Sie „Check Point“ im Dropdown-Menü **Typ (Type)** aus.

c Geben Sie das primäre VPN-Gateway (und das sekundäre VPN Gateway, falls erforderlich) ein.

d Klicken Sie auf **Weiter (Next)**.

Es wird ein Dialogfeld für Ihre Non VMware SD-WAN Site angezeigt (siehe Abbildung unten).



Hinweis Um Tunneleinstellungen für das primäre VPN-Gateway der Non VMware SD-WAN Site zu konfigurieren, klicken Sie auf die erweiterte Schaltfläche, die sich am unteren Rand des Dialogfelds befindet. Alle Änderungen, die an „Verschlüsselung (Encryption)“, „DH-Gruppe (DH Group)“ oder „PFS“ vorgenommen wurden, werden auch auf die redundante Tunnelkonfiguration angewendet. Aktualisieren Sie nach dem Speichern Ihrer Änderungen das primäre VPN-Gateway-Gerät der Site. Klicken Sie auf die Optionsschaltfläche „IKE/IPSec-Vorlage anzeigen (View IKE/IPSec Template)“.

4 Geben Sie im Bereich „Primäres VPN-Gateway (Primary VPN Gateway)“ Folgendes ein:

a **PSK**: Geben Sie den vorinstallierten Schlüssel ein, der auf dem Check Point-Infinity-Portal konfiguriert wurde. Konfigurieren Sie keine redundanten IPSec-Tunnel (behalten Sie die Aktivierung des Kontrollkästchens **Redundantes VeloCloud-Cloud-VPN (Redundant VeloCloud Cloud VPN)** bei).

b **Verschlüsselung (Encryption)**: Die Verschlüsselung sollte auf denselben Algorithmus festgelegt werden, der im Check Point-Infinity-Portal konfiguriert wurde.

c **DH-Gruppe (DH Group)**: Die DH-Gruppe sollte auf denselben Wert festgelegt werden, der im Check Point-Infinity-Portal konfiguriert wurde.

d Für die Zwecke dieser spezifischen Check Point-Konfiguration wählen Sie aus dem PFS-Dropdown-Menü die Option **deaktiviert (disabled)** aus.

5 Um ein sekundäres VPN-Gateway hinzuzufügen, klicken Sie auf die Schaltfläche **Hinzufügen (Add)**. Wenn Sie auf die Schaltfläche **Änderungen speichern (Save Changes)** klicken, wird das sekundäre VPN-Gateway für diese Site sofort erstellt und diesem Gateway wird ein VMware SD-WAN-VPN-Tunnel bereitgestellt.

Hinweis Bei einer Non VMware SD-WAN Site vom Typ Check Point wird die öffentliche IP der SD-WAN Gateway-Schnittstelle standardmäßig als Wert für die lokale Authentifizierungs-ID verwendet.

6 Wie in Schritt 4a oben erwähnt, behalten Sie die Aktivierung des Kontrollkästchens **Redundantes VeloCloud-Cloud-VPN (Redundant VeloCloud Cloud VPN)** bei.

7 Wählen Sie für die Zwecke der Check Point-Konfiguration die Option **Standard** aus dem Dropdown-Menü „Lokale Authentifizierungs-ID (Local Auth Id)“ aus.

8 Aktivieren Sie zum Zweck der Check Point-Konfiguration das Kontrollkästchen **Site-Subnetze deaktivieren (Disable Site Subnets)**.

9 Klicken Sie auf **Änderungen speichern (Save Changes)**.

10 Aktivieren Sie das Kontrollkästchen **Tunnel aktivieren (Enable Tunnel(s))**, sobald Sie bereit sind, den Tunnel vom SD-WAN Gateway zu den Check Point-CloudGuard-VPN-Gateways zu initiieren.

Konfigurieren von Zscaler

Die Zscaler-Konfiguration umfasst vier Hauptschritte. Sie müssen alle vier Schritte ausführen, um diese Konfiguration abzuschließen.

Die ersten drei Hauptschritte umfassen das Einrichten eines VPN-IPSec-Tunnel-Gateways zwischen VMware SD-WAN und Zscaler, und der letzte Schritt erfordert die Einrichtung von Geschäftsregeln. Führen Sie die folgenden Konfigurationsschritte aus:

1 Erstellen und konfigurieren Sie eine Non VMware SD-WAN Site.

2 Fügen Sie dem Konfigurationsprofil eine Non VMware SD-WAN Site hinzu.

3 Zscaler-Konfiguration: Erstellen Sie ein Konto, fügen Sie VPN-Anmeldedaten hinzu und fügen Sie einen Speicherort hinzu.

4 Konfigurieren Sie Geschäftsprioritätsregeln.

Hinweis Sie führen Schritt 1, Schritt 2 und Schritt 4 in SD-WAN Orchestrator aus. Sie führen Schritt 3 auf der Zscaler-Website durch.

Erstellen und Konfigurieren einer Non VMware SD-WAN Site

So erstellen und konfigurieren Sie eine Non VMware SD-WAN Site:

1 Klicken Sie im Navigationsbereich auf **Konfigurieren (Configure) > Netzwerkdienste (Network Services)**.

Der Bildschirm **Dienste (Services)** wird angezeigt.

2 Klicken Sie im Bereich **Nicht-VeloCloud-Sites (Non-VeloCloud Sites)** auf die Schaltfläche **Neu (New)**.

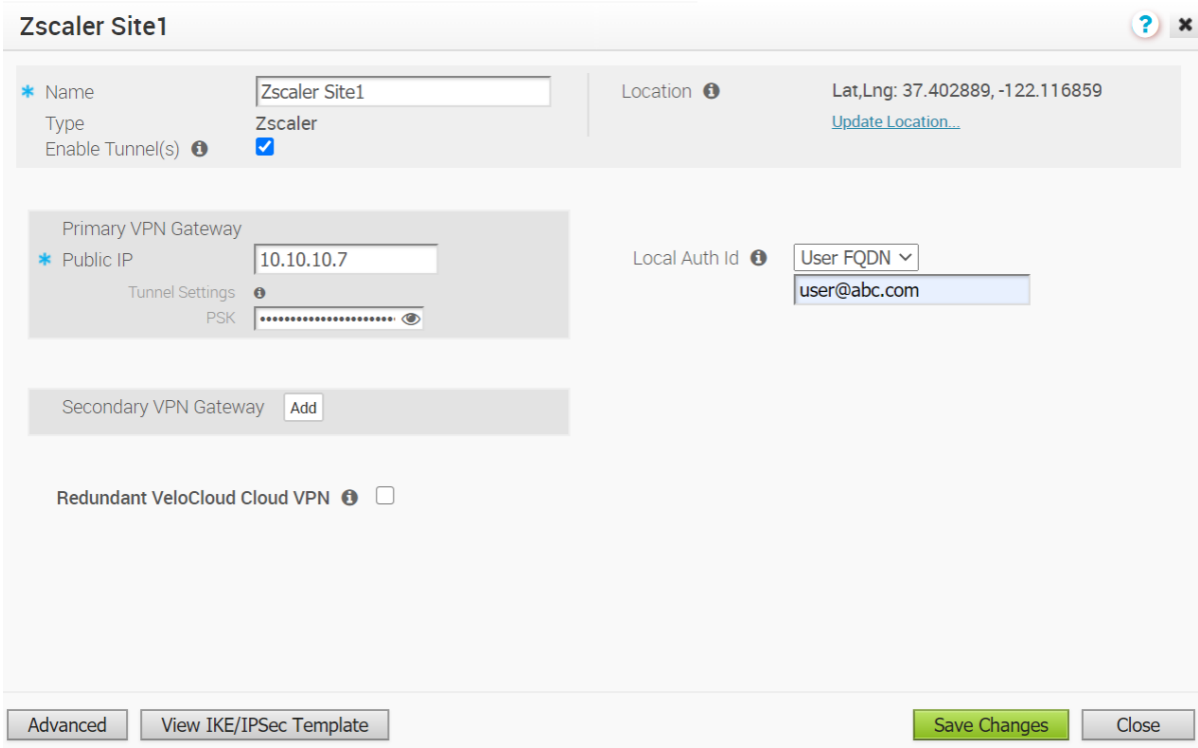
Das Dialogfeld **Neue Nicht-VeloCloud-Site (New Non-VeloCloud Site)** wird angezeigt.

3 Gehen Sie im Dialogfeld **Neue Nicht-VeloCloud-Site (New Non-VeloCloud Site)** wie folgt vor:

a Geben Sie im Textfeld **Name** den Namen für die Non VMware SD-WAN Site ein.

b Wählen Sie im Dropdown-Menü **Typ (Type)** den Eintrag **Zscaler** aus.

c Geben Sie die IP-Adresse für das primäre VPN-Gateway (und bei Bedarf für das sekundäre VPN-Gateway) an und klicken Sie auf **Weiter (Next)**. Eine Non VMware SD-WAN Site vom Typ Zscaler wird erstellt und ein Dialogfeld für Ihre Non VMware SD-WAN Site wird angezeigt.



4 Gehen Sie im Dialogfeld für Ihre Non VMware SD-WAN Site wie folgt vor:

a Um die Tunneleinstellungen für das primäre VPN-Gateway der Non VMware SD-WAN Site zu konfigurieren, klicken Sie auf die Schaltfläche **Erweitert (Advanced)**.

b Im Bereich **Primäres VPN-Gateway (Primary VPN Gateway)** unter **Tunneleinstellungen (Tunnel Settings)** können Sie den vorinstallierten Schlüssel (Pre-Shared Key, PSK) konfigurieren. Hierbei handelt es sich um den Sicherheitsschlüssel für die Authentifizierung über den Tunnel. Der Orchestrator generiert standardmäßig einen PSK. Wenn Sie einen eigenen PSK oder ein eigenes Kennwort verwenden möchten, können Sie dies in das Textfeld eingeben.

c Wenn Sie ein sekundäres VPN-Gateway für diese Site erstellen möchten, klicken Sie auf die Schaltfläche **Hinzufügen (Add)** neben **Sekundäres VPN-Gateway (Secondary VPN Gateway)**. Geben Sie im Popup-Fenster die IP-Adresse des sekundären VPN-Gateways ein und klicken Sie auf **Änderungen speichern (Save Changes)**. Das sekundäre VPN-Gateway wird sofort für diese Site erstellt und stellt einen VMware SD-WAN-VPN-Tunnel für dieses Gateway bereit.

d Aktivieren Sie das Kontrollkästchen **Redundantes VeloCloud-Cloud-VPN (Redundant VeloCloud Cloud VPN)**, um redundante Tunnel für jedes VPN-Gateway hinzuzufügen. Alle Änderungen, die am PSK des primären VPN-Gateways vorgenommen wurden, werden, falls konfiguriert, auch auf die redundanten VPN-Tunnel angewendet. Nachdem Sie die Tunneleinstellungen des primären VPN-Gateways geändert haben, speichern Sie die Änderungen und klicken dann auf **IKE/IPSec-Vorlage anzeigen (View IKE/IPSec Template)**, um die aktualisierte Tunnelkonfiguration anzuzeigen.

e Klicken Sie auf den Link **Standort aktualisieren (Update location)**, um den Standort für die konfigurierte Non VMware SD-WAN Site anzuzeigen. Die Angaben zum Längen- und Breitengrad werden verwendet, um den besten Edge oder das beste Gateway zu bestimmen, mit dem eine Verbindung im Netzwerk hergestellt werden kann.

f Mit der lokalen Authentifizierungs-ID werden das Format und die Identifizierung des lokalen Gateways festgelegt. Wählen Sie im Dropdown-Menü**Lokale Authentifizierungs-ID (Local Auth Id)** unter den folgenden Typen und geben Sie einen ermittelten Wert ein:

- **FQDN**: Der vollqualifizierte Domänenname oder der Hostname. Beispiel: google.com.
- **Benutzer-FQDN (User FQDN)**: Der vollqualifizierte Domänenname in Form einer E-Mail-Adresse. Beispiel: user@google.com.
- **IPv4**: Die zur Kommunikation mit dem lokalen Gateway verwendete IP-Adresse.

Hinweis Für eine Non VMware SD-WAN Site vom Typ Zscaler wird empfohlen, den FQDN oder den Benutzer-FQDN als lokale Authentifizierungs-ID zu verwenden.

Kopieren Sie die lokalen Authentifizierungsdetails und das PSK-Kennwort. (Sie benötigen diese Informationen, wenn Sie Ihre VPN-Anmeldedaten in Ihrem Zscaler-Konto einrichten).

g Aktivieren Sie das Kontrollkästchen **Tunnel aktivieren (Enable Tunnel(s))**, sobald Sie bereit sind, den Tunnel vom SD-WAN Gateway zu den Zscaler-VPN-Gateways zu initiieren.

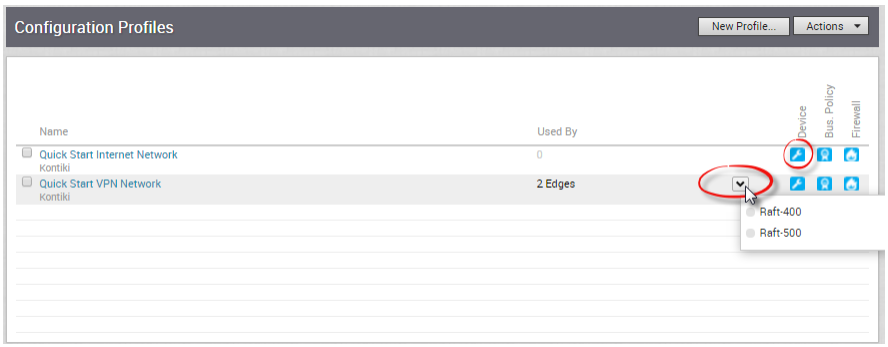
h Klicken Sie auf **Änderungen speichern (Save Changes)**.

Verknüpfen einer NVS mit einem Konfigurationsprofil

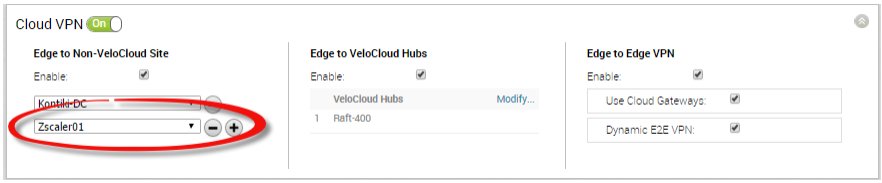
So verknüpfen Sie eine NVS mit einem Konfigurationsprofil:

1 Klicken Sie im Navigationsfenster auf **Konfigurieren (Configure) > Profile (Profiles)**.

2 Klicken Sie auf der Seite **Profile konfigurieren (Configure Profiles)** rechts neben Ihrem Profil auf das Symbol **Geräte (Devices)** . (Verwenden Sie für mehrere Edges das Dropdown-Menü, um Ihren Edge auszuwählen, und klicken Sie dann auf die Registerkarte **Gerät (Device)**.)



3 Klicken Sie im Bereich **Cloud-VPN (Cloud VPN)** auf das Symbol ⊕ und wählen Sie Ihre Non VMware SD-WAN Site aus dem Dropdown-Menü aus.



Hinweis Sie können auch eine neue Non VMware SD-WAN Site im Cloud-VPN-Bereich erstellen. Nachdem Sie auf das Symbol ⊕ geklickt haben, wählen Sie im Dropdown-Menü den Eintrag **Neue Nicht-VeloCloud-Site (New Non-VeloCloud Site)** aus.

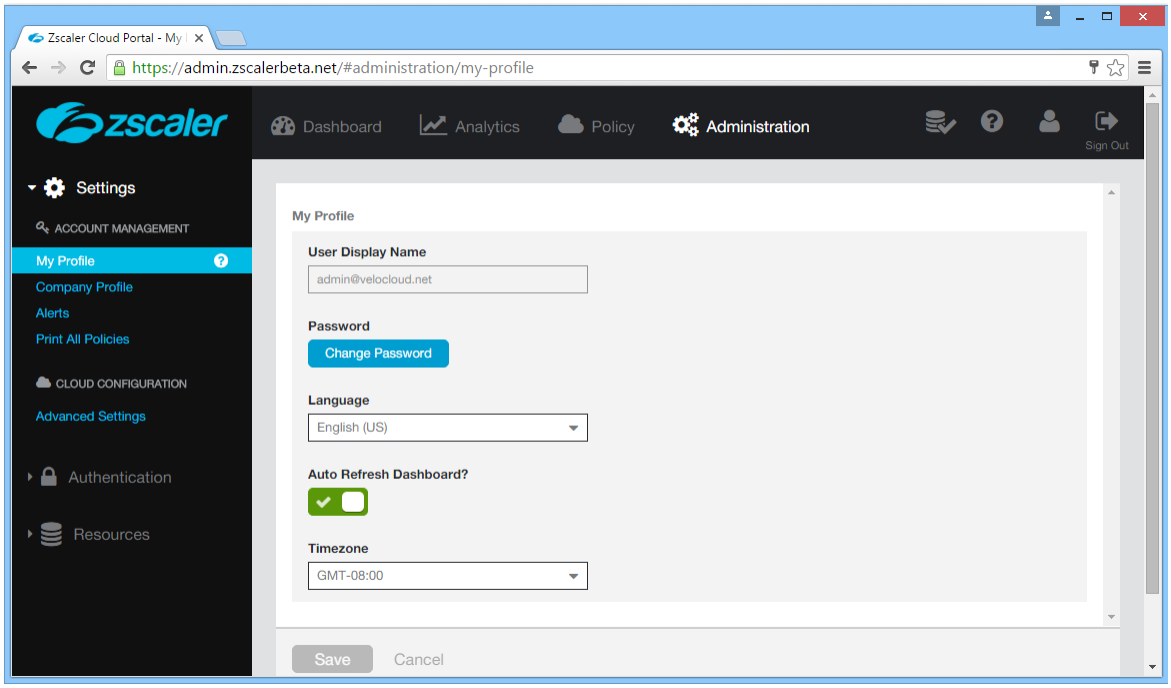
4 Klicken Sie auf **Änderungen speichern (Save Changes)**.

Konfigurieren von Zscaler

In diesem Abschnitt wird die Konfiguration von Zscaler beschrieben.

Führen Sie die folgenden Schritte auf der Zscaler-Website aus. Dort erstellen Sie ein Zscaler-Konto, fügen die VPN-Anmeldedaten hinzu und fügen einen Speicherort hinzu.

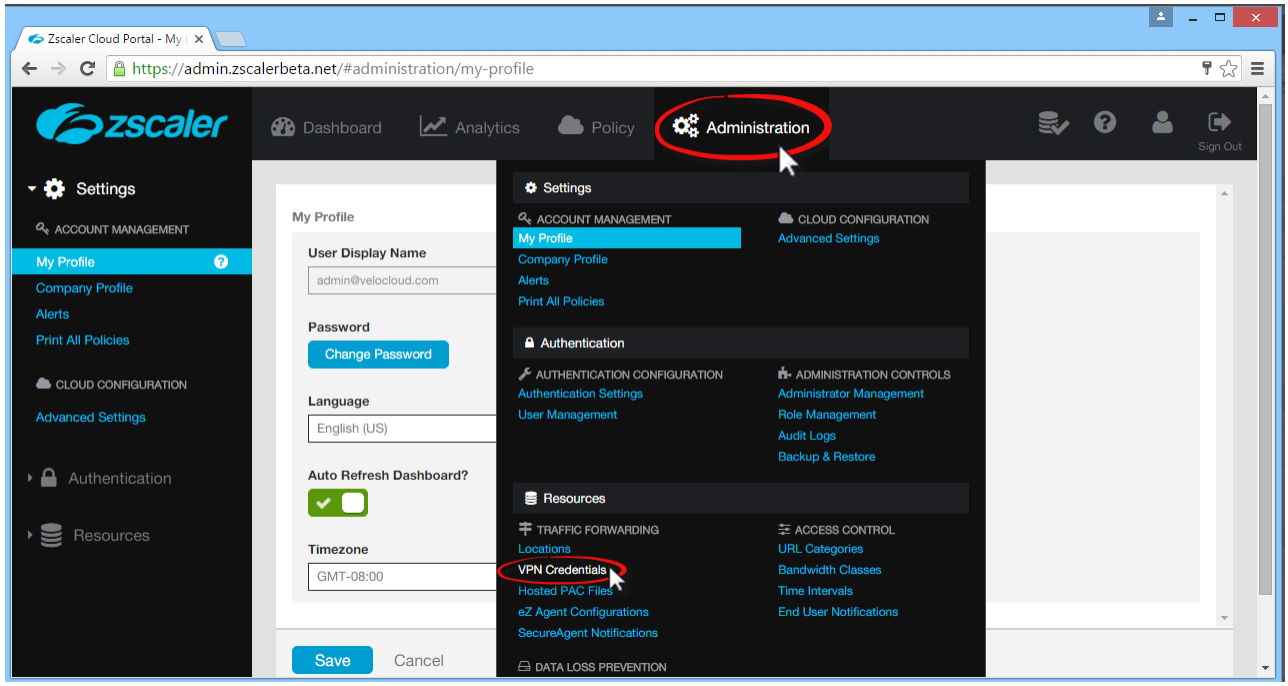
1 Erstellen Sie auf der Website von Zscaler ein Zscaler-Websicherheitskonto.



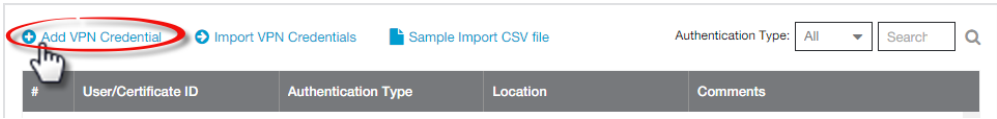
2 Richten Sie Ihre VPN-Anmeldedaten ein:

a Bewegen Sie oben im Zscaler-Bildschirm den Mauszeiger über die Option **Verwaltung (Administration)**, um das Dropdown-Menü anzuzeigen. (Siehe Abbildung unten.)

b Klicken Sie unter **Ressourcen (Resources)** auf **VPN-Anmeldedaten (VPN Credentials)**.



c Klicken Sie in der oberen linken Ecke auf **VPN-Anmeldedaten hinzufügen (Add VPN Credentials)**.

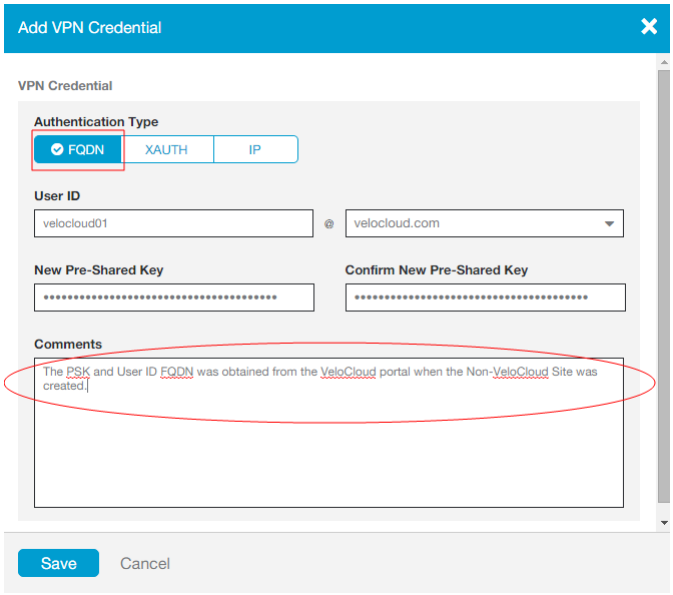


d Gehen Sie im Dialogfeld **VPN-Anmeldedaten hinzufügen (Add VPN Credential)** wie folgt vor:

1 Wählen Sie **FQDN** als Authentifizierungstyp aus.

2 Geben Sie die Benutzer-ID und den vorinstallierten Schlüssel (Pre-Shared Key, PSK) ein. Diese Informationen erhalten Sie aus Ihrem Non VMware SD-WAN Site-Dialogfeld in SD-WAN Orchestrator.

3 Geben Sie bei Bedarf Kommentare im Abschnitt **Kommentare (Comments)** ein.



4 Klicken Sie auf **Speichern (Save)**.

3 Weisen Sie einen Speicherort zu:

a Bewegen Sie oben im Zscaler-Bildschirm den Mauszeiger über die Option **Verwaltung (Administration)**, um das Dropdown-Menü anzuzeigen.

b Klicken Sie unter **Ressourcen (Resources)** auf **Standorte (Locations)**.

c Klicken Sie in der oberen linken Ecke auf **Standort hinzufügen (Add Location)**.

d Gehen Sie im Dialogfeld **Standort hinzufügen (Add Location)** wie folgt vor (siehe Abbildung unten):

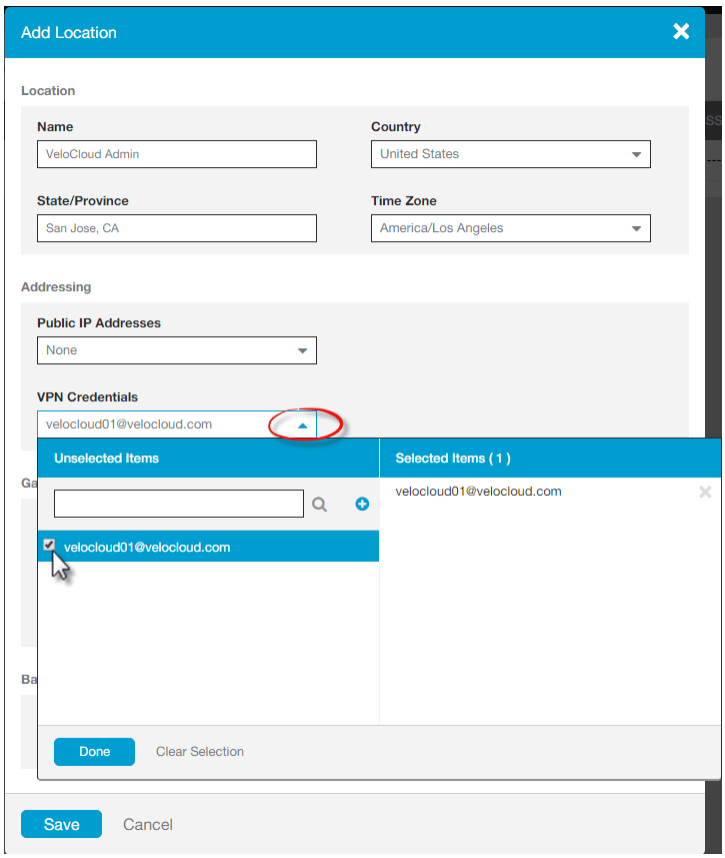
1 Füllen Sie die Textfelder (Name, Land, Bundesland/Kanton, Zeitzone) im Bereich für den Standort aus.

2 Wählen Sie im Dropdown-Menü **Öffentliche IP-Adressen (Public IP Addresses)** die Option **Keine (None)** aus.

3 Wählen Sie im Dropdown-Menü **VPN-Anmeldedaten (VPN Credentials)** die soeben erstellten Anmeldedaten aus. (Siehe Abbildung unten.)

4 Klicken Sie auf **Fertig (Done)**.

5 Klicken Sie auf **Speichern (Save)**.



Konfigurieren von Geschäftsprioritätsregeln

Definieren Sie die Unternehmensrichtlinie in Ihrem SD-WAN Orchestrator, um die Überprüfung der Websicherheit zu ermitteln.

1 Gehen Sie im Navigationsbereich in SD-WAN Orchestrator zu **Konfigurieren (Configure) > Edges**.

2 Klicken Sie im Bildschirm **Edges** auf das Symbol **Unternehmensrichtlinie (Bus. Policy)** für Ihren Edge.

3 Klicken Sie auf die Schaltfläche **Neue Regel (New Rule)**.

   a Im Dialogfeld **Regel (Rule)**:

      1 Geben Sie einen Namen für die Regel in das Textfeld **Regelname (Rule Name)** ein.

      2 Wählen Sie im Bereich **Ziel (Destination)** des Abschnitts **Übereinstimmung (Match)** die gewünschten Optionen aus. (Beispieloptionen werden unten angezeigt.)

         a Klicken Sie auf die Schaltfläche **Definieren (Define)**.

         b Wählen Sie **Internet** aus.

         c Wählen Sie **TCP** im Dropdown-Menü **Protokoll (Protocol)** aus.

d Geben Sie den Port in das Textfeld **Ports** ein. Die folgende Abbildung zeigt ein Beispiel, bei dem der Port 80 verwendet wird. VMware SD-WAN empfiehlt die Verwendung von Port 80 oder Port 443. Weitere Informationen finden Sie im Hinweis am Ende dieses Abschnitts.

3 Wählen Sie im Bereich **Aktion (Action)** Ihre Optionen aus. (Beispieloptionen werden unten angezeigt.)

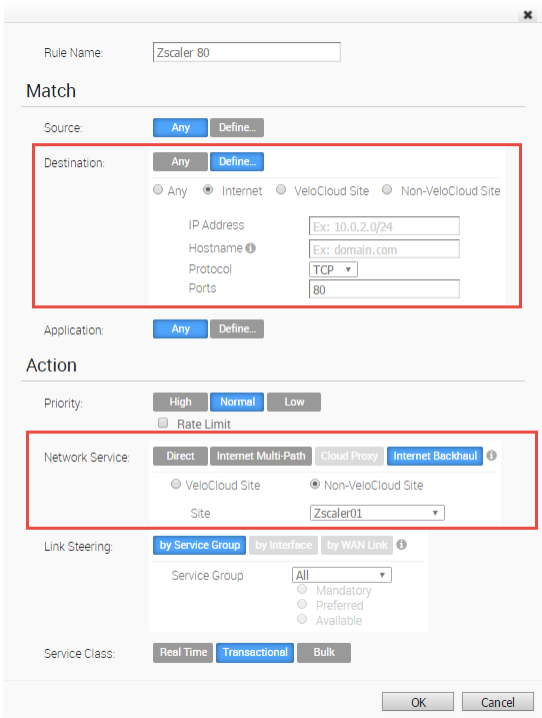
a Wählen Sie für **Priorität (Priority)** die Option **Normal** aus.

b Klicken Sie für **Netzwerkdienst (Network Service)** auf **Internet-Backhaul (Internet Backhaul)** und wählen Sie im Dropdown-Menü Ihre Non VMware SD-WAN Site aus.

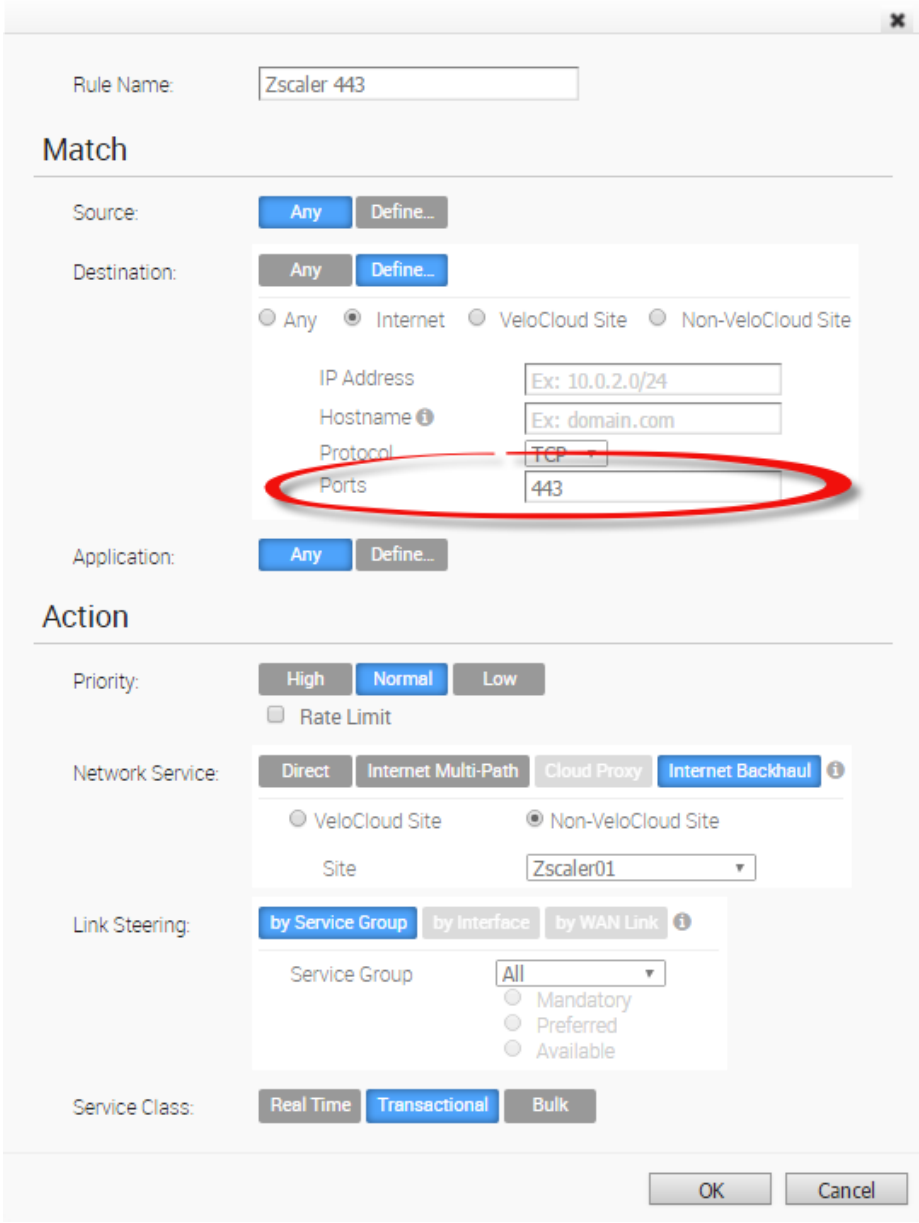
c Wählen Sie für **Link-Steuerung (Link Steering)** eine Option aus (z. B. **Nach Dienstgruppe (by Service Group)**).

d Wählen Sie für **Dienstklasse (Service Class)** die Option **Transaktional (Transactional)** aus.

b Klicken Sie auf **OK**.



Hinweis VMware SD-WAN empfiehlt Regeln für Unternehmensrichtlinien für Backhaul-Webdatenverkehr, insbesondere Port 80 und Port 443. Sie können den gesamten Internetdatenverkehr an Backhaul Zscaler senden. Ein Beispiel, in dem Port 443 verwendet wird, ist in der folgenden Abbildung dargestellt.



Konfigurieren von Amazon Web Services

VMware SD-WAN unterstützt die Konfiguration von Amazon Web Services (AWS) in Non VMware SD-WAN Site.

Konfigurieren Sie Amazon Web Services (AWS) wie folgt:

1 Rufen Sie die Details zu „Öffentliche IP (Public IP)“, „Interne IP (Inside IP)“ und „PSK“ von der Amazon Web Services-Website ab.

2 Geben Sie die von der AWS-Website abgerufenen Informationen in den Nicht-VMware SD-WAN-Netzwerkdienst in der VMware SD-WAN Orchestrator-Instanz ein.

Um die Konfiguration mit Amazon Web Services vorzunehmen, führen Sie die Schritte im folgenden Abschnitt aus.

Abrufen von Konfigurationsdetails für Amazon Web Services

In diesem Abschnitt wird beschrieben, wie Sie die Konfigurationsdetails für Amazon Web Services abrufen.

Wenn Sie Amazon Web Services für Ihre Konfigurationen verwenden, lesen Sie die Anweisungen in der Dokumentation von Amazon (Amazon Virtual Private Cloud Network Administrator Guide). Sie finden diese unter: http://awsdocs.s3.amazonaws.com/VPC/latest/vpc-nag.pdf. Im Abschnitt „Beispiel: Generisches Kunden-Gateway ohne Border Gateway“ auf Seite 79 finden Sie spezifische Konfigurationsanweisungen.

1 Erstellen Sie über Amazon Web Services VPC- und VPN-Verbindungen. (Im Abschnitt oben finden Sie den Link, über den Sie auf Amazon Web Services zugreifen können, um diesen Schritt durchzuführen.)

2 Notieren Sie sich das SD-WAN Gateways, das mit dem Unternehmenskonto in SD-WAN Orchestrator verbunden ist, und gegebenenfalls benötigt wird, um ein virtuelles privates Gateway in Amazon Web Services zu erstellen.

3 Notieren Sie sich die öffentliche IP, die innere IP und die PSK-Details, die dem Virtual Private Gateway zugeordnet sind. Diese Informationen geben Sie in SD-WAN Orchestrator ein, wenn Sie eine Non VMware SD-WAN Site erstellen.

Erstellen und Konfigurieren einer Non VMware SD-WAN Site

Nachdem Sie die öffentliche IP, die innere IP und die PSK-Informationen von der Website von Amazon Web Services (AWS) erhalten haben, können Sie eine Non VMware SD-WAN Site konfigurieren.

So konfigurieren Sie eine Non VMware SD-WAN Site:

1 Navigieren Sie zu **Konfigurieren (Configure) > Netzwerkdienste (Network Services)**.

2 Klicken Sie im Bereich **Nicht-VeloCloud-Sites (Non-VeloCloud Sites)** auf die Schaltfläche **Neu (New)**.

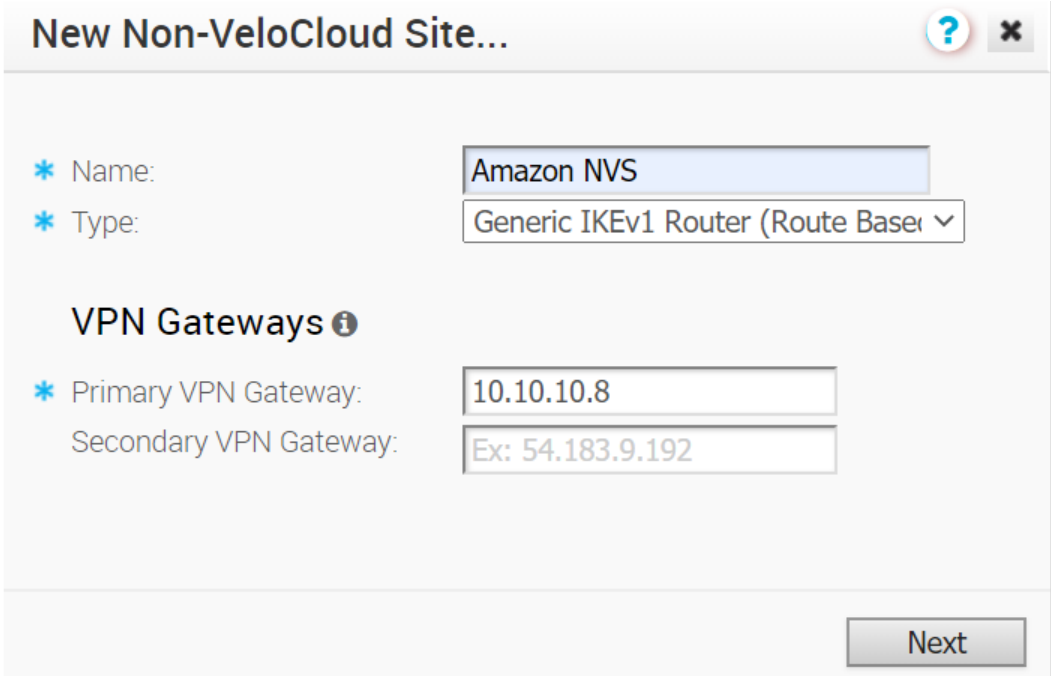
3 Gehen Sie im Dialogfeld **Neue Nicht-VeloCloud-Site (New Non-VeloCloud Site)** wie folgt vor:

   a Geben Sie den Name Ihrer Site ein.

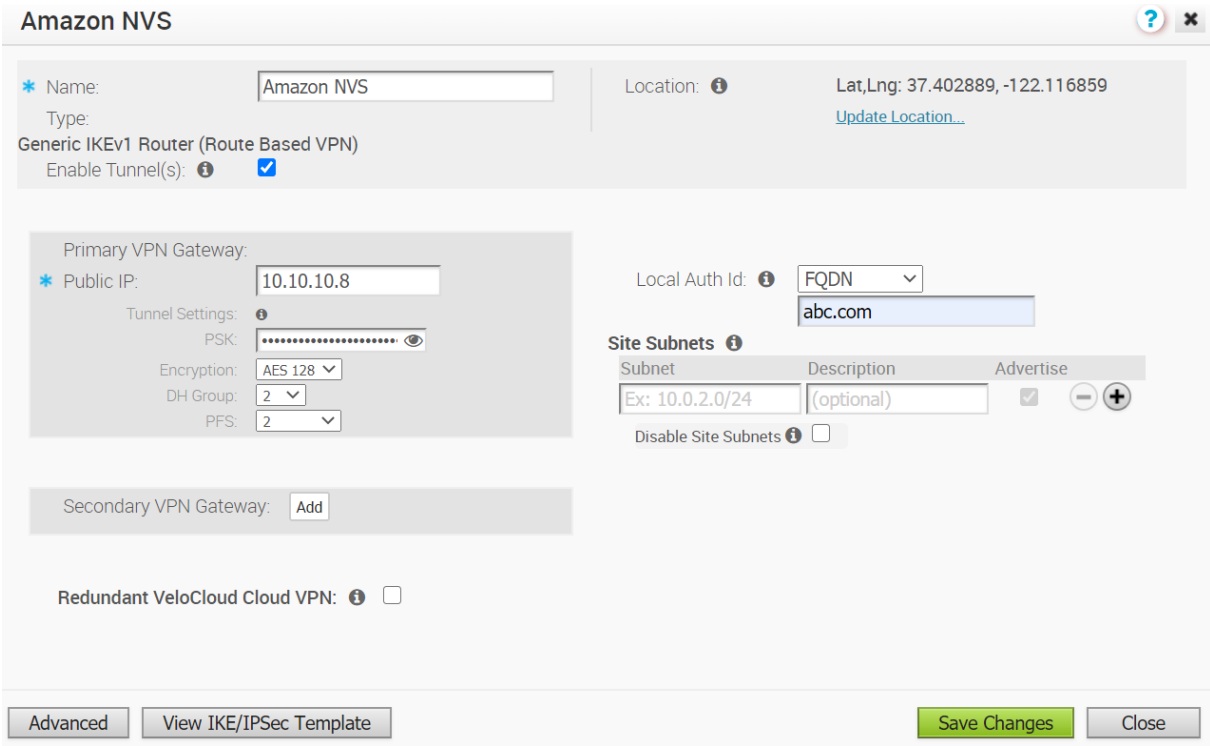
   b Wählen Sie aus dem Dropdown-Menü **Typ (Type)** die Option **Generischer IKEv1-Router (routenbasiertes VPN) (Generic IKEv1 Router (Route Based VPN))** oder **Generischer IKEv2-Router (routenbasiertes VPN) (Generic IKEv2 Router (Route Based VPN))** aus.

   c Geben Sie das primäre VPN-Gateway (und das sekundäre VPN Gateway, falls erforderlich) ein.

   d Klicken Sie auf **Weiter (Next)**.



Eine routenbasierte Non VMware SD-WAN Site wird erstellt und ein Dialogfeld für Ihre Non VMware SD-WAN Site wird angezeigt.



4 Um die Tunneleinstellungen für das primäre VPN-Gateway der Non VMware SD-WAN Site zu konfigurieren, klicken Sie auf die Schaltfläche **Erweitert (Advanced)**.

5 Im Bereich **Primäres VPN-Gateway (Primary VPN Gateway)** können Sie die folgenden Tunneleinstellungen konfigurieren:

Feld	Beschreibung
PSK	Der vorinstallierte Schlüssel (Pre-Shared Key, PSK), der der Sicherheitsschlüssel für die Authentifizierung über den Tunnel ist. Der Orchestrator generiert standardmäßig einen PSK. Wenn Sie einen eigenen PSK oder ein eigenes Kennwort verwenden möchten, können Sie dies in das Textfeld eingeben.
Verschlüsselung (Encryption)	Wählen Sie entweder **AES 128** oder **AES 256** als Algorithmus zum Verschlüsseln von Daten aus. Der Standardwert ist AES 128.
DH-Gruppe (DH Group)	Wählen Sie den Diffie-Hellman (DH)-Gruppen-Algorithmus aus, der beim Austausch eines vorinstallierten Schlüssels verwendet werden soll. Über die DH-Gruppe wird die Stärke des Algorithmus in Bit festgelegt. Der Standardwert ist 2.
PFS	Wählen Sie die PFS-Ebene (Perfect Forward Secrecy) für zusätzliche Sicherheit aus. Der Standardwert ist 2.

6 Wenn Sie ein sekundäres VPN-Gateway für diese Site erstellen möchten, klicken Sie auf die Schaltfläche **Hinzufügen (Add)** neben **Sekundäres VPN-Gateway (Secondary VPN Gateway)**. Geben Sie im Popup-Fenster die IP-Adresse des sekundären VPN-Gateways ein und klicken Sie auf **Änderungen speichern (Save Changes)**.

Das sekundäre VPN-Gateway wird sofort für diese Site erstellt und stellt einen VMware SD-WAN-VPN-Tunnel für dieses Gateway bereit.

7 Aktivieren Sie das Kontrollkästchen **Redundantes VeloCloud-Cloud-VPN (Redundant VeloCloud Cloud VPN)**, um redundante Tunnel für jedes VPN-Gateway hinzuzufügen.

Alle Änderungen, die an „Verschlüsselung (Encryption)“, „DH-Gruppe (DH Group)“ oder „PFS von Primäres VPN-Gateway (PFS of Primary VPN Gateway)“ vorgenommen wurden, werden, falls konfiguriert, auch auf die redundanten VPN-Tunnel angewendet. Nachdem Sie die Tunneleinstellungen des primären VPN-Gateways geändert haben, speichern Sie die Änderungen und klicken dann auf **IKE/IPSec-Vorlage anzeigen (View IKE/IPSec Template)**, um die aktualisierte Tunnelkonfiguration anzuzeigen.

8 Klicken Sie auf den Link **Standort aktualisieren (Update location)**, um den Standort für die konfigurierte Non VMware SD-WAN Site anzuzeigen. Die Angaben zum Längen- und Breitengrad werden verwendet, um den besten Edge oder das beste Gateway zu bestimmen, mit dem eine Verbindung im Netzwerk hergestellt werden kann.

9 Mit der lokalen Authentifizierungs-ID werden das Format und die Identifizierung des lokalen Gateways festgelegt. Wählen Sie im Dropdown-Menü**Lokale Authentifizierungs-ID (Local Auth Id)** unter den folgenden Typen und geben Sie einen ermittelten Wert ein:

- **FQDN**: Der vollqualifizierte Domänenname oder der Hostname. Beispiel: google.com.

- **Benutzer-FQDN (User FQDN)**: Der vollqualifizierte Domänenname in Form einer E-Mail-Adresse. Beispiel: user@google.com.
- **IPv4**: Die zur Kommunikation mit dem lokalen Gateway verwendete IP-Adresse.

Hinweis Wenn der Benutzer bei Auswahl von generischem routenbasierten VPN keinen Wert angibt, wird **Standard (Default)** als lokale Authentifizierungs-ID verwendet. Als Standardwert der lokalen Authentifizierungs-ID wird die öffentliche IP der SD-WAN Gateway-Schnittstelle verwendet.

10 Unter **Site-Subnetze (Site Subnets)** können Sie Subnetze für die Non VMware SD-WAN Site hinzufügen, indem Sie auf die Schaltfläche mit dem Pluszeichen (**+**) klicken. Wenn Sie keine Subnetze für die Site benötigen, aktivieren Sie das Kontrollkästchen **Site-Subnetze deaktivieren (Disable Site Subnets)**.

11 Aktivieren Sie das Kontrollkästchen **Tunnel aktivieren (Enable Tunnel(s))**, sobald Sie bereit sind, den Tunnel vom SD-WAN Gateway zu den Gateways des generischen Router-VPN zu initiieren.

12 Klicken Sie auf **Änderungen speichern (Save Changes)**.

Konfigurieren von Cloud-Sicherheitsdiensten

Der Cloud-Sicherheitsdienst ist ein in der Cloud gehostetes Sicherheitsangebot (z. B. Firewalls, URL-Filterung usw.) Dies schützt die Zweigstelle und/oder das Datencenter eines Unternehmens. In den folgenden Abschnitten wird beschrieben, wie Sie eine Instanz eines Cloud-Sicherheitsdienstes definieren und konfigurieren und wie Sie einen sicheren Tunnel direkt vom Edge zum Cloud-Sicherheitsdienst einrichten.

Übersicht über die Cloud-Sicherheitsdienste

Dieser Abschnitt bietet einen Überblick über die Cloud-Sicherheitsdienste.

Zurzeit wird die Verbindungskonnektivität von einem Zweigstellen-Edge zu einem Cloud-Dienst oder einer Non VMware SD-WAN Site über das SD-WAN Gateway hergestellt. In diesem Modell aggregiert das SD-WAN Gateway den Datenverkehr von mehreren Zweigstellen-Edges und leitet den Datenverkehr sicher an die Non VMware SD-WAN Site weiter.

Sie können den Zweigstellen-Edge auch so konfigurieren, dass ein Tunnel direkt zum Cloud-Dienst-PoP hergestellt wird. Diese Option bietet folgende Vorteile:

- Sie können Kosten für die Verbindungsbandbreite sparen, indem Sie den nicht für das Unternehmen spezifischen Datenverkehr in das Internet verlagern.
- Indem Sie den Internetverkehr zu einem Cloud-Sicherheitsdienst umleiten, können Sie sicherstellen, dass die Zweigstellen-Websites vor bösartigem Datenverkehr geschützt sind.
- Vereinfachte Konfiguration.

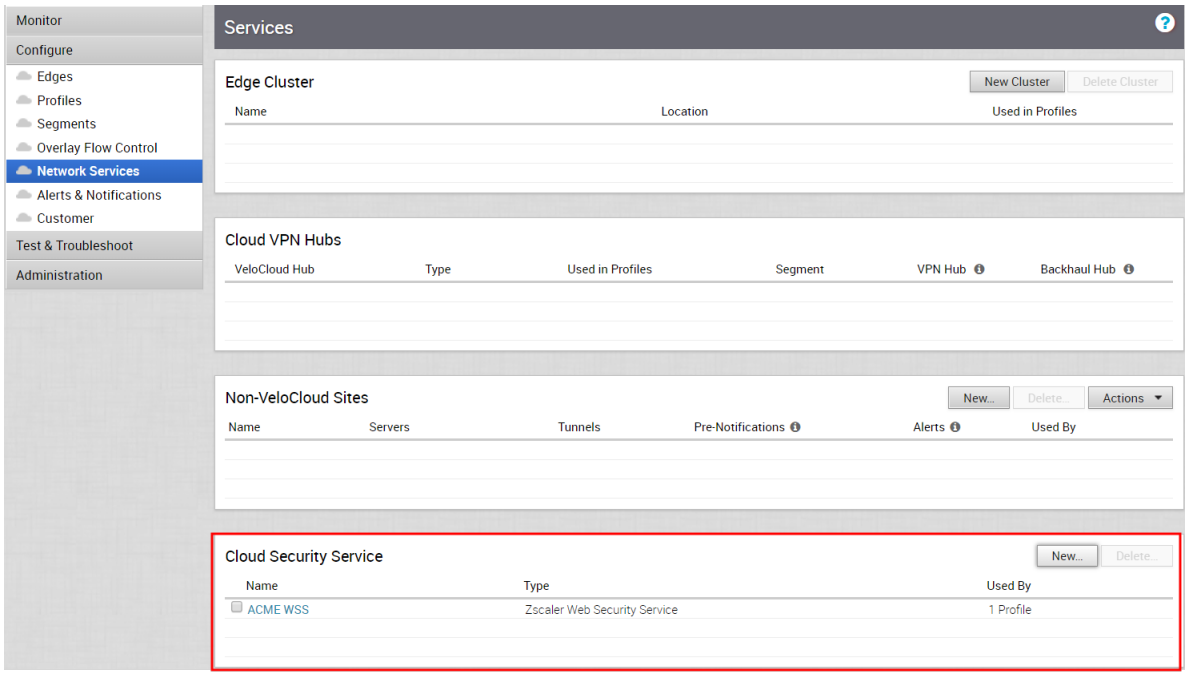
In diesem Dokument wird beschrieben, wie Sie eine Instanz eines Cloud-Sicherheitsdienstes definieren und konfigurieren und einen sicheren Tunnel direkt vom Edge zum Cloud-Sicherheitsdienst einrichten. Die Konfiguration besteht aus drei Teilen:

- Konfigurieren von Cloud-Sicherheitsdiensten
- Konfigurieren von Cloud-Sicherheitsdiensten für Profile
- Konfigurieren von Cloud-Sicherheitsdiensten für Edges

Konfigurieren von Cloud-Sicherheitsdiensten

Sie können die Cloud-Sicherheitsdienste über das Fenster „Netzwerkdienste“ (Network Services) konfigurieren.

Navigieren Sie im Unternehmensportal zu **Konfigurieren (Configure) > Netzwerkdienste (Network Services)**. Sie können die Dienstinstanz im Bereich **Cloud-Sicherheitsdienst (Cloud Security Service)** festlegen, um einen sicheren Tunnel zu den Cloud-Sicherheitsdienst-Sites über den Edge zu erstellen.



Hinzufügen und Konfigurieren eines Cloud Security Provider

Der Cloud-Sicherheitsdienst stellt einen sicheren Tunnel von einem Edge zu den Cloud-Sicherheitsdienst-Sites her. Dadurch wird sichergestellt, dass der Datenverkehr für die Cloud-Sicherheitsdienste gesichert ist.

1 Klicken Sie im Fenster „Kunde (Customer)“ auf **Konfigurieren (Configure) > Netzwerkdienste (Network Services)**.

2 Klicken Sie im Fenster **Cloud-Sicherheitsdienst (Cloud Security Service)** auf **Neu (New)**.

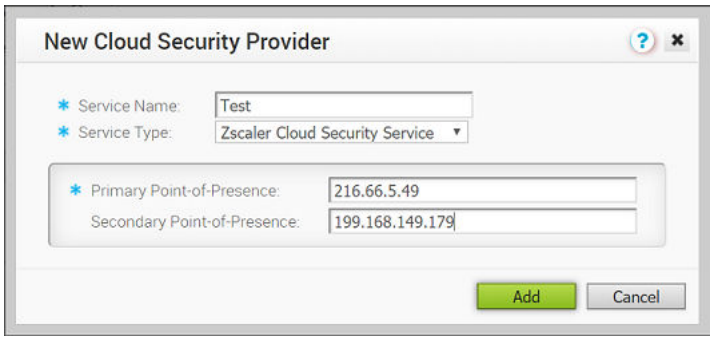
3 Wählen Sie im Dialogfeld **Neuer Cloud Security Provider (New Cloud Security Provider)** den **Diensttyp (Service Type)** für den Cloud-Dienst aus.

4 Geben Sie einen beschreibenden Namen neben **Dienstname (Service Name)** ein.

5 Geben Sie eine IP-Adresse unter **Primärer Point-of-Presence/Server (Primary Point-of-Presence/Server)** und **Sekundärer Point-of-Presence/Server (Secondary Point-of-Presence/Server)** ein.

Hinweis Wenn Sie **Zscaler Cloud Security Service** als Diensttyp ausgewählt haben und die Zuweisung eines GRE-Tunnels planen, wird empfohlen, als Point-of-Presence nur die IP-Adresse und nicht den Hostnamen einzugeben, da GRE keine Hostnamen unterstützt.

6 Um Ihre Konfiguration zu bearbeiten, klicken Sie auf **Hinzufügen (Add)**.



Hinweis Sie müssen die Tunnelattribute für die einzelnen Edges konfigurieren. Weitere Informationen finden Sie im Abschnitt Konfigurieren von Cloud-Sicherheitsdiensten für Edges.

Konfigurieren von Cloud-Sicherheitsdiensten für Profile

Sie müssen die Cloud-Sicherheit aktivieren, um einen sicheren Tunnel von einem Edge zu Cloud-Sicherheitsdienst-Sites einzurichten. Dadurch kann der gesicherte Datenverkehr an die Cloud-Sicherheits-Sites von Drittanbietern umgeleitet werden.

Bevor Sie beginnen:

- Stellen Sie sicher, dass Sie über Zugriffsberechtigungen zum Konfigurieren der Netzwerkdienste verfügen.
- Stellen Sie sicher, dass Ihr SD-WAN Orchestrator die Version 3.3.x oder höher aufweist.
- Die Endpoint-IPs und FQDN-Zugangsdaten des Cloud-Sicherheitsdienst-Gateways sollten im CSS des Drittanbieters konfiguriert sein.

1 Klicken Sie im Unternehmensportal auf **Konfigurieren (Configure) > Profile (Profiles)**.

2 Klicken Sie auf das Gerätesymbol neben einem Profil oder klicken Sie auf den Link zum Profil und dann auf die Registerkarte **Gerät (Device)**.

3 Schalten Sie im Abschnitt **Cloud-Sicherheit (Cloud Security)** den Wählschalter von der Position **Aus (Off)** in die Position **Ein (On)**.

4 Konfigurieren Sie die folgenden Einstellungen:

Option	Beschreibung
Cloud-Sicherheitsdienst (Cloud Security Service)	Wählen Sie im Dropdown-Menü einen Cloud-Sicherheitsdienst aus. Sie können im Dropdown-Menü auch auf **Neuer Cloud-Sicherheitsdienst (New Cloud Security Service)** klicken, um einen neuen Diensttyp zu erstellen.
Tunnelprotokoll (Tunneling Protocol)	Diese Option ist nur für den Zscaler-Cloud-Sicherheitsdienst verfügbar. Wählen Sie entweder „IPSec“ oder „GRE“ aus. Standardmäßig ist „IPsec“ ausgewählt.
Hash	Wählen Sie als Hash-Funktion „SHA 1“ oder „SHA 256“ in der Dropdown-Liste aus. Standardmäßig ist „SHA 1“ ausgewählt. **Hinweis** VMware SD-WAN unterstützt MD5 nicht und es wird empfohlen, MD5 nicht als Hash-Funktion zu wählen.
Verschlüsselung (Encryption)	Wählen Sie als Verschlüsselungsalgorithmus „AES 128“ oder „AES 256“ in der Dropdown-Liste aus. Standardmäßig ist „Keine (None)“ ausgewählt.
Schlüsselaustauschprotokoll (Key Exchange Protocol)	Diese Option ist für den Symantec-Cloud-Sicherheitsdienst nicht verfügbar. Wählen Sie als Schlüsselaustauschmethode „IKEv1“ oder „IKEv2“ aus. Standardmäßig ist „IKEv2“ ausgewählt.

5 Klicken Sie auf **Änderungen speichern (Save Changes)**.

Wenn Sie den Cloud-Sicherheitsdienst aktivieren und die Einstellungen in einem Profil konfigurieren, wird die Einstellung automatisch auf die Edges angewendet, die mit dem Profil verknüpft sind. Falls erforderlich, können Sie die Konfiguration für einen bestimmten Edge außer Kraft setzen. Weitere Informationen finden Sie unter Konfigurieren von Cloud-Sicherheitsdiensten für Edges.

Für die Profile, die mit vor Version 3.3.1 aktivierten und konfigurierten Cloud-Sicherheitsdiensten erstellt wurden, kann der Datenverkehr wie folgt umgeleitet werden:

- Nur Webdatenverkehr an Cloud-Sicherheitsdienst umleiten
- Gesamten internetgebundenen Datenverkehr an Cloud-Sicherheitsdienst umleiten

- Datenverkehr basierend auf Unternehmensrichtlinieneinstellungen umleiten – Diese Option ist erst ab Version 3.3.1 verfügbar. Bei Auswahl dieser Option stehen die beiden anderen Optionen nicht länger zur Verfügung.

Hinweis Für die neuen Profile, die Sie für Version 3.3.1 oder höher erstellt haben, wird der Datenverkehr standardmäßig gemäß der Unternehmensrichtlinieneinstellungen umgeleitet.

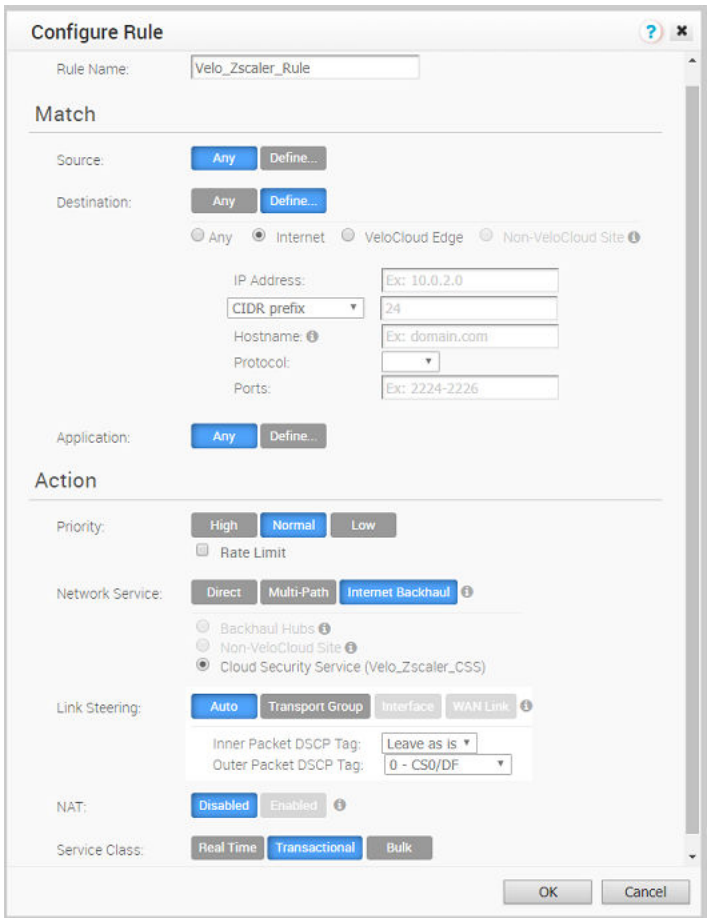
Zum Umleiten des Datenverkehrs zum Cloud-Sicherheitsdienst können Sie eine Regel in der Unternehmensrichtlinie erstellen.

1 Erstellen Sie auf der Registerkarte **Unternehmensrichtlinie (Business Policy)** des Profils eine neue Regel, indem Sie auf **Neue Regel (New Rule)** klicken oder im Dropdown-Menü **Aktionen (Actions)** die Option **Neu (New)** auswählen.

Das Dialogfeld **Regel konfigurieren (Configure Rule)** wird angezeigt.

2 Geben Sie einen eindeutigen Namen unter **Regelname (Rule Name)** ein.

3 Klicken Sie im Bereich **Aktion (Action)** auf die Schaltfläche **Internet-Backhaul (Internet Backhaul)** und wählen Sie **Cloud-Sicherheitsdienst (Cloud Security Service)** aus.



4 Klicken Sie auf **OK**.

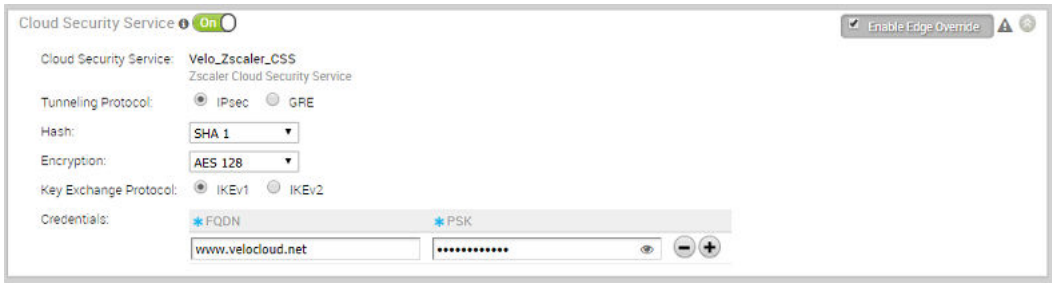
Die neue Regel wird auf der Seite **Unternehmensrichtlinie (Business Policy)** angezeigt.

Konfigurieren von Cloud-Sicherheitsdiensten für Edges

Wenn Sie einem Edge ein Profil zugewiesen haben, erbt das Gerät automatisch den mit dem Profil verknüpften Cloud-Sicherheitsdienst. Sie können die Einstellungen überschreiben, um die Attribute für jeden Edge zu ändern.

1 Klicken Sie im Unternehmensportal auf **Konfigurieren (Configure) > Edges**.

2 Im Abschnitt **Cloud-Sicherheitsdienst (Cloud Security Service)** werden die Cloud-Sicherheitsdienstparameter des zugehörigen Profils angezeigt. Klicken Sie auf **Edge-Außerkraftsetzung aktivieren (Enable Edge Override)**, um die Attribute zu ändern. Weitere Informationen zu den Attributen finden Sie unter Konfigurieren von Cloud-Sicherheitsdiensten für Profile.



Neben den vorhandenen Attributen können Sie die folgenden zusätzlichen Parameter für einen Edge konfigurieren:

- **FQDN** – Geben Sie den vollständig qualifizierten Domänennamen für ein IPsec-Protokoll ein.
- **PSK** – Geben Sie den vorinstallierten Schlüssel für ein IPsec-Protokoll ein.

Hinweis Die oben genannten Optionen sind für den Cloud-Sicherheitsdienst Symantec nicht verfügbar.

Wenn Sie das GRE-Tunneling-Protokoll für den Cloud-Sicherheitsdienst Zscaler auswählen, müssen Sie die GRE-Tunnel-Parameter hinzufügen.

1 Klicken Sie auf **Tunnel hinzufügen (Add Tunnel)**.

2 Konfigurieren Sie im Fenster **Tunnel hinzufügen (Add Tunnel)** die folgenden Einstellungen:

Option	Beschreibung
WAN-Links (WAN Links)	Wählen Sie die WAN-Schnittstelle aus, die vom GRE-Tunnel als Quelle verwendet werden soll.
Öffentliche IP-Adresse der Tunnelquelle (Tunnel Source Public IP)	Wählen Sie die IP-Adresse aus, die vom Tunnel als öffentliche IP-Adresse verwendet werden soll. Sie können entweder „WAN-Link-IP (WAN Link IP)“ oder „Benutzerdefinierte WAN-IP (Custom WAN IP)“ auswählen. Wenn Sie „Benutzerdefinierte WAN-IP (Custom WAN IP)“ auswählen, geben Sie die IP-Adresse ein, die als öffentliche IP verwendet werden soll.
Primäre Router-IP/-Maske (Primary Router IP/Mask)	Geben Sie die primäre IP-Adresse des Routers ein.
Sekundäre Router-IP/-Maske (Secondary Router IP/Mask)	Geben Sie die sekundäre IP-Adresse des Routers ein.
Primäre ZEN-IP/-Maske (Primary ZEN IP/Mask)	Geben Sie die primäre IP-Adresse des internen Edge für den öffentlichen Zscaler-Dienst ein.
Sekundäre ZEN-IP/-Maske (Secondary ZEN IP/Mask)	Geben Sie die sekundäre IP-Adresse des internen Edge für den öffentlichen Zscaler-Dienst ein.

Hinweis Die Router-IP/-Maske und die ZEN-IP/-Maske werden von Zscaler bereitgestellt.

3 Klicken Sie auf **OK**, und die Tunneldetails werden im Abschnitt „Cloud-Sicherheitsdienste (Cloud Security Services)“ angezeigt.

Klicken Sie im Fenster **Edges** auf **Änderungen speichern (Save Changes)**, um die geänderten Einstellungen zu speichern.

Für die Profile, die mit vor Version 3.3.1 aktivierten und konfigurierten Cloud-Sicherheitsdiensten erstellt wurden, kann der Datenverkehr wie folgt umgeleitet werden:

- Nur Webdatenverkehr an Cloud-Sicherheitsdienst umleiten
- Gesamten internetgebundenen Datenverkehr an Cloud-Sicherheitsdienst umleiten
- Datenverkehr basierend auf Unternehmensrichtlinieneinstellungen umleiten – Diese Option ist erst ab Version 3.3.1 verfügbar. Bei Auswahl dieser Option stehen die beiden anderen Optionen nicht länger zur Verfügung.

Hinweis Für die neuen Profile, die Sie für Version 3.3.1 oder höher erstellt haben, wird der Datenverkehr standardmäßig gemäß der Unternehmensrichtlinieneinstellungen umgeleitet.

Zum Verknüpfen des Cloud-Sicherheitsdiensts können Sie eine Regel in der Unternehmensrichtlinie erstellen.

1 Erstellen Sie auf der Registerkarte **Unternehmensrichtlinie (Business Policy)** des Edge eine neue Regel, indem Sie auf **Neue Regel (New Rule)** klicken oder im Dropdown-Menü **Aktionen (Actions)** die Option **Neue Regel (New Rule)** auswählen.

   Das Dialogfeld **Regel konfigurieren (Configure Rule)** wird angezeigt.

2 Geben Sie einen eindeutigen Namen unter **Regelname (Rule Name)** ein.

3 Klicken Sie im Bereich **Aktion (Action)** auf die Schaltfläche **Internet-Backhaul (Internet Backhaul)** und wählen Sie **Cloud-Sicherheitsdienst (Cloud Security Service)** aus.

4 Klicken Sie auf **OK**.

   Die neue Regel wird auf der Seite **Unternehmensrichtlinie (Business Policy)** angezeigt.

Überwachen von Cloud-Sicherheitsdiensten

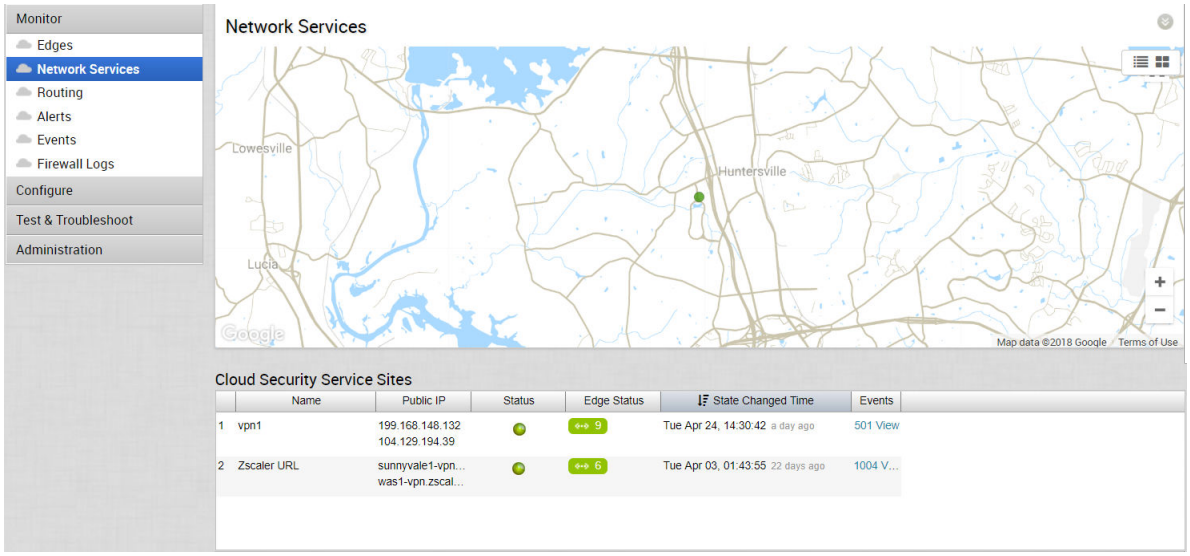
Cloud-Sicherheitsdienste können an zwei Stellen im Navigationsbereich überwacht werden: im Bildschirm **Edges** (**Überwachen (Monitor) > Edges**) und im Bildschirm **Netzwerkdienste (Network Services)** (**Überwachen (Monitor) > Netzwerkdienste (Network Services)**). In den folgenden Abschnitten finden Sie weitere Informationen.

Bildschirm „Edges“

Zum Überwachen der Cloud-Dienste über den Bildschirm **Edges** navigieren Sie zu **Überwachen (Monitor) > Edges**. In dieser Ansicht wird die Anzahl der offenen und geschlossenen Tunnel angezeigt.

Bildschirm „Netzwerkdienste“ (Network Services)

Um Ihre Cloud-Sicherheitsdienste über den Bildschirm **Netzwerkdienste (Network Services)** zu überwachen, navigieren Sie zu **Überwachen > Netzwerkdienste > Tunnelstatus für Cloud-Sicherheit (Monitor > Network Services > Cloud Security Tunnel State)**.



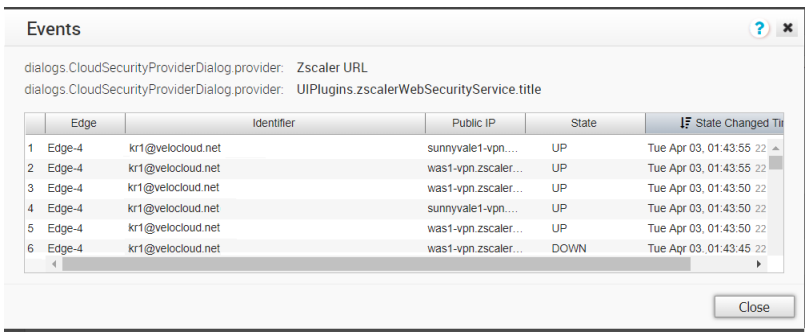
Die Spalte „Edge-Status“ (Edge Status) im Bereich „Tunnelstatus für Cloud-Sicherheit“ (Cloud Security Tunnel State) zeigt, wie viele Edges vollständig verbunden sind und wie viele getrennt sind.

Spalte „Status“

In der Spalte **Status** wird der Gesamtkonnektivitätsstatus des jeweiligen Cloud-Sicherheitsdiensts angezeigt. Wenn alle Edges vollständig verbunden sind, wird die Farbe des Symbols grün. Wenn nur einige Edges verbunden sind, andere hingegen getrennt, wird die Farbe des Symbols gelb. Wenn alle Edges getrennt sind, wird die Farbe des Symbols rot.

Ereignisse

Um die Ereignisse für den Cloud-Sicherheitsdienst anzuzeigen, klicken Sie auf den Link **Ereignisse (Events)** im Bereich **Cloud-Sicherheitsdienst-Sites (Cloud Security Service Sites)**.

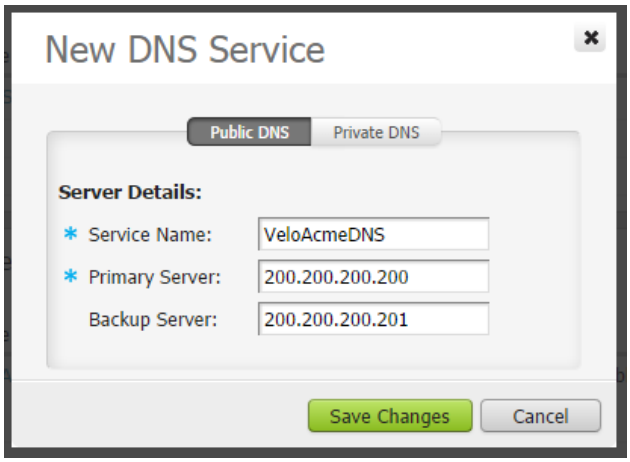


Konfigurieren von DNS-Diensten

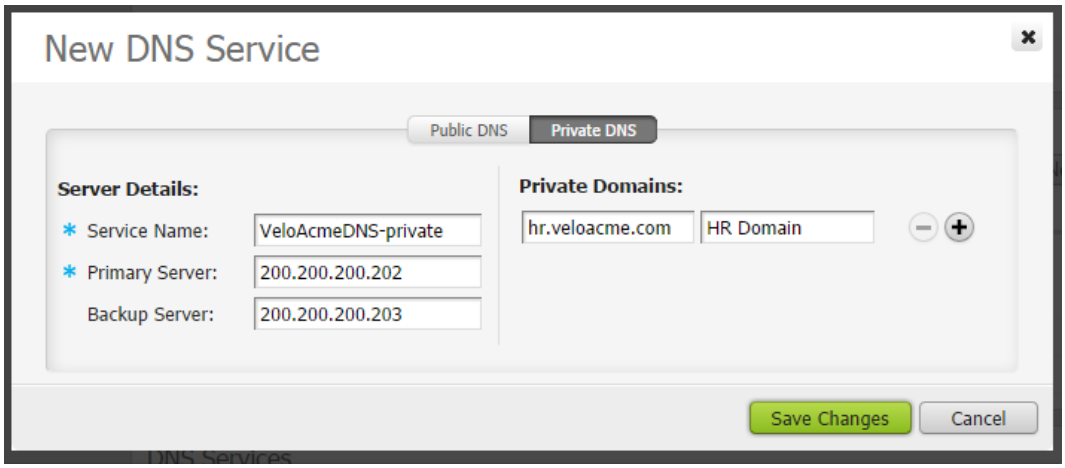
Hierbei handelt es sich um einen optionalen Dienst, mit dem Sie eine Konfiguration für DNS erstellen können.

Der DNS-Server kann für einen öffentlichen DNS-Server oder einen privaten DNS-Server verwendet werden, der von Ihrem Unternehmen bereitgestellt wird. Es kann ein **Primärserver (Primary Server)** und **Sicherungsserver (Backup Server)** angegeben werden. Der Dienst ist für die Verwendung von Google und die Open DNS-Server vorkonfiguriert.

Die folgende Abbildung zeigt eine Beispielkonfiguration für einen öffentlichen DNS.



Für einen privaten Dienst können Sie auch eine oder mehrere **Private Domänen (Private Domains)** angeben.



Konfigurieren von Netflow-Einstellungen

In einem Unternehmensnetzwerk überwacht NetFlow den Datenverkehr, der über SD-WAN Edges geleitet wird, und exportiert IPFIX-Informationen (Internet Protocol Flow Information eXport) direkt aus SD-WAN Edges in eine oder mehrere NetFlow-Collector-Instanzen. Mit SD-WAN Orchestrator können Sie NetFlow-Collector-Instanzen und Filter als Netzwerkdienste auf der Profil-, Edge- und Segmentebene konfigurieren. Sie können maximal zwei Collector-Instanzen pro Segment und acht Collector-Instanzen pro Profil und Edge konfigurieren. Darüber hinaus können Sie maximal 16 Filter pro Collector konfigurieren.

Verfahren

1 Navigieren Sie in der SD-WAN Orchestrator-Instanz zur Option **Konfigurieren (Configure)** > **Netzwerkdienste (Network Services)**.

   Die Seite **Dienste (Services)** wird angezeigt.

2 Um einen Collector zu konfigurieren, navigieren Sie zum Bereich **Netflow-Einstellungen (Netflow Settings)** und klicken Sie auf der rechten Seite der Tabelle „Collector“ auf die Schaltfläche **Neu (New)**. Das Dialogfeld **Neuen Collector hinzufügen (Add New Collector)** wird angezeigt.

   a Geben Sie im Textfeld **Collector-Name (Collector Name)** einen eindeutigen Namen für den Collector ein.

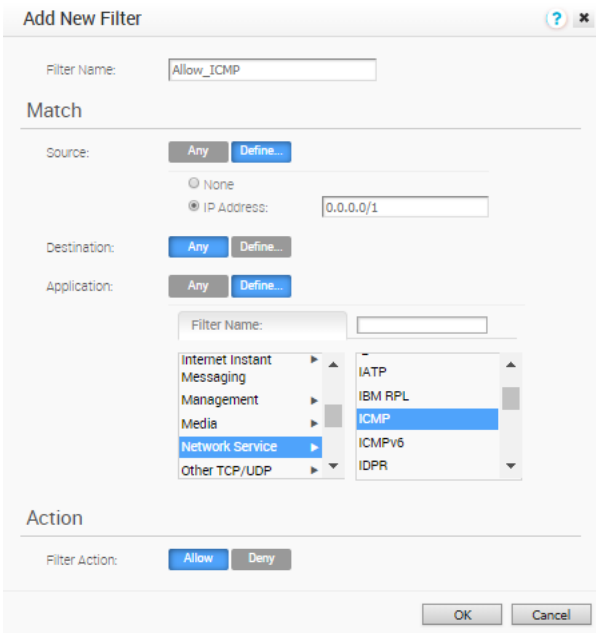
   b Geben Sie im Textfeld **Collector-IP (Collector IP)** die IP-Adresse des Collectors ein.

   c Geben Sie im Textfeld **Collector-Port (Collector Port)** die Port-ID des Collectors ein.

   d Klicken Sie auf **Änderungen speichern (Save Changes)**.

      Unter **Netzwerkdienste (Network Services)** wird der neu hinzugefügte Collector in der Tabelle „Collector“ angezeigt.

3 SD-WAN Orchestrator ermöglicht das Filtern von Datenverkehrs-Flow-Datensätzen nach Quell-IP, Ziel-IP und Anwendungs-ID, die mit dem Flow verbunden sind. Um einen Filter zu konfigurieren, navigieren Sie zum Bereich **Netflow-Einstellungen (Netflow Settings)** und klicken Sie auf der Schaltfläche auf der rechten Seite der Tabelle „Filter“ auf **Neu (New)**. Das Dialogfeld **Neuen Filter hinzufügen (Add New Filter)** wird angezeigt.



a Geben Sie im Textfeld **Filtername (Filter Name)** einen eindeutigen Anzeigenamen für den Filter ein.

b Klicken Sie im Bereich **Übereinstimmung (Match)** auf **Definieren (Define)**, um Filterregeln pro Collector zu definieren, die nach Quell-IP oder Ziel-IP oder Anwendung, die mit dem Datenfluss verknüpft sind, übereinstimmen, oder klicken Sie auf **Alle (Any)**, um eine der Quell-IPs oder Ziel-IPs oder Anwendungen, die mit dem Datenfluss verknüpft sind, als Übereinstimmungskriterium für die Netflow-Filterung zu verwenden.

c Wählen Sie im Bereich **Aktion (Action)** entweder **Zulassen (Allow)** oder **Verweigern (Deny)** als Filteraktion für den Datenverkehrsfluss aus und klicken Sie auf **OK**.

Unter **Netzwerkdienste (Network Services)** wird der neu gezeigte Filter in der Tabelle „Filter“ angezeigt.

Ergebnisse

Auf der Profil- und Edge-Ebene werden die konfigurierten Collector-Instanzen und die Filter als Liste unter dem Bereich **Einstellungen (Settings)** auf der Registerkarte **Gerät (Device)** angezeigt.

- Beim Konfigurieren eines Profils oder Edge können Sie entweder einen Collector auswählen und aus der verfügbaren Liste filtern oder einen neuen Collector und einen Filter hinzufügen. Die Schritte dazu finden Sie unter Konfigurieren von Netflow-Einstellungen auf der Profilebene.

- Informationen zum Überschreiben der NetFlow-Einstellungen auf der Edge-Ebene finden Sie unter Konfigurieren der Netflow-Einstellungen auf der Edge-Ebene.

Private Netzwerknamen

Sie können mehrere private Netzwerke definieren und sie einzelnen privaten WAN-Overlays zuweisen.

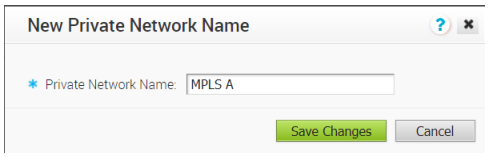
Konfigurieren von privaten Netzwerken

So konfigurieren Sie private Netzwerke:

1 Navigieren Sie im SD-WAN Orchestrator-Navigationsbereich zu **Konfigurieren (Configure) > Netzwerkdienste (Network Services)**.

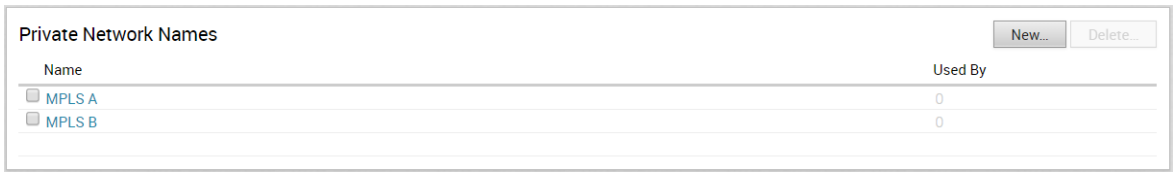
2 Klicken Sie im Bereich **Private Netzwerknamen (Private Network Names)** auf die Schaltfläche **Neu (New)**.

3 Geben Sie im Dialogfeld **Neuer privater Netzwerkname (New Private Network Name)** einen eindeutigen Vornamen in das entsprechende Textfeld ein.



4 Klicken Sie auf **Änderungen speichern (Save Changes)**.

Der private Netzwerkname wird im Bereich **Privater Netzwerkname (Private Network Name)** angezeigt.



Löschen eines privaten Netzwerknamens

Nur private Netzwerknamen, die nicht von einem Edge-Gerät verwendet werden, können gelöscht werden.

So löschen Sie einen privaten Netzwerknamen, der nicht von einem Edge-Gerät verwendet wird:

1 Wählen Sie den Namen aus, indem Sie das dazugehörige Kontrollkästchen aktivieren, und klicken Sie dann auf Schaltfläche **Löschen (Delete)**.

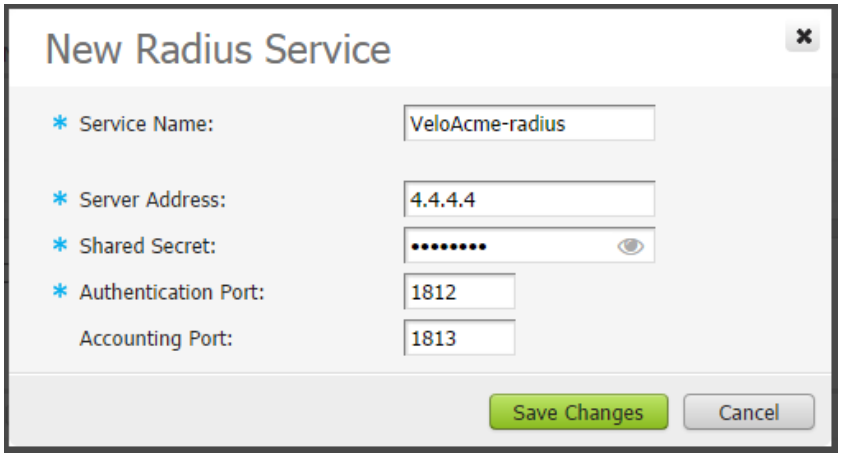
2 Klicken Sie im **Dialogfeld „Löschen bestätigen (Confirm Delete)“** auf **OK**.

Sie können private Link-Tags auswählen, wenn Sie ein benutzerdefiniertes Overlay definieren. Weitere Informationen finden Sie im Abschnitt *Auswählen eines privaten Netzwerknamens*.

Konfigurieren von Authentifizierungsdiensten

Authentifizierungsdienste sind eine optionale Konfiguration. Wenn Ihre Organisation einen Dienst für die Authentifizierung oder Buchhaltung verwendet, können Sie einen Netzwerkdienst erstellen, der die IP-Adresse und die Ports für den Dienst angibt. Dies ist ein Teil des 802.1x-Konfigurationsvorgangs, der im Profil konfiguriert wird.

Die folgende Abbildung zeigt eine Beispielkonfiguration.



Konfigurieren von Profilen 9

Profile stellen eine Zusammenstellung der in Netzwerken und Netzwerkdiensten erstellten Konfigurationen dar. Außerdem werden mit Profilen Konfigurationen für Unternehmensrichtlinien und Firewallregeln hinzugefügt.

Hinweis Wenn Sie mit einer Benutzer-ID angemeldet sind, die über Kundensupport-Berechtigungen verfügt, können Sie nur SD-WAN Orchestrator-Objekte anzeigen. Sie werden nicht in der Lage sein, neue Objekte zu erstellen oder bestehende zu konfigurieren/aktualisieren.

Profile haben vier Registerkarten: **Profilübersicht (Profile Overview)**, **Gerät (Device)**, **Unternehmensrichtlinie (Business Policy)** und **Firewall**.

Dieses Kapitel enthält die folgenden Themen:

- Erstellen eines Profils
- Ändern eines Profils
- Bildschirm „Profilübersicht“ (Profile Overview)
- Migration von Netzwerk zu Segment
- Konfigurieren lokaler Anmeldedaten

Erstellen eines Profils

Nach einer neuen Installation verfügt die SD-WAN Orchestrator-Instanz über die folgenden vordefinierten Profile: Internetprofil, VPN-Profil und ab Version 3.0 segmentbasierte Profile.

Hinweis Da die Segmentierung in Version 3.0 eingeführt wurde, können Edges, auf denen eine Softwareversion vor Version 3.0 ausgeführt wird, über eine netzwerkbasierte Konfiguration oder eine segmentierungsbasierte Konfiguration verfügen. ****Aufgrund dieses Übergangs müssen Sie das netzwerkbasierte Profil in das segmentbasierte Profil migrieren/umwandeln.**

Die folgenden Schritte werden in der Regel bei der Erstellung eines neuen Profils befolgt:

1 Erstellen eines Profils

2 Gerät konfigurieren

   a Netzwerk auswählen

b Authentifizierung/DNS zuweisen

c Benutzeroberflächeneinstellungen konfigurieren

3 Cloud-VPN aktivieren

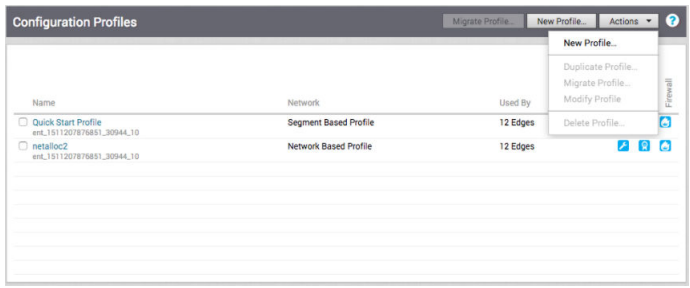
4 Unternehmensrichtlinie konfigurieren

5 Konfigurieren der Firewall

6 Profilübersicht überprüfen

So erstellen Sie ein neues Profil:

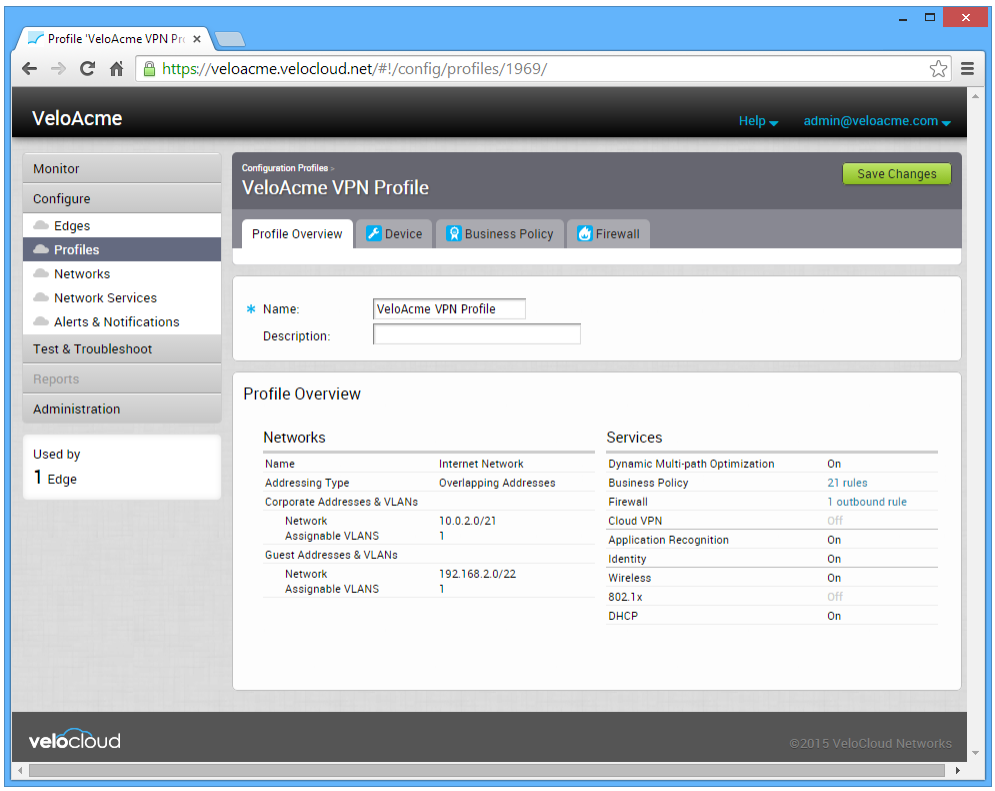
1 Navigieren Sie zu „Konfigurieren (Configure) -> Profile (Profiles)“ und klicken Sie auf die Schaltfläche **Neues Profil (New Profile)**.



2 Geben Sie im Dialogfeld **Neues Profil (New Profile)** einen Profilnamen und eine Beschreibung in die entsprechenden Textfelder ein.

3 Klicken Sie auf die Schaltfläche **Erstellen (Create)**.

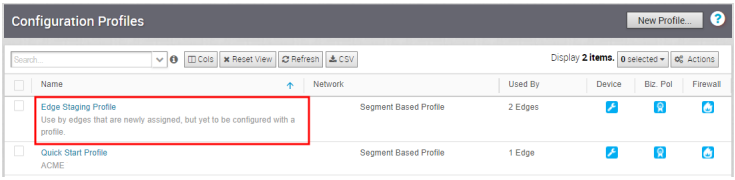
Die Seite **Profilübersicht (Profile Overview)** wird aktualisiert. Weitere Informationen finden Sie im folgenden Abschnitt **Profilübersicht (Profile Overview) Bildschirm (Screen)**.



Ändern eines Profils

Unternehmensadministratoren können einem Edge auch manuell ein Profil zuweisen.

Ein Szenario, in dem dies notwendig ist, ist für Edge-Bereitstellungsprofile. In diesem Fall wird der Edge aufgrund einer Übertragung per Push standardmäßig anhand des Bereitstellungsprofils aktiviert. Unternehmensadministratoren müssen dem Edge manuell ein endgültiges Produktionsprofil zuweisen. Weitere Informationen zum manuellen Zuweisen von Profilen finden Sie unter *Bereitstellen eines Edge* in *Zuweisen eines Profils (Ändern eines Profils)*.



Bildschirm „Profilübersicht“ (Profile Overview)

Der Bildschirm **Profilübersicht (Profile Overview)** bietet eine schnelle Übersicht über alle in diesem Profil definierten Netzwerke und Dienste.

Die Übersicht ist in zwei Kategorien unterteilt:

Kategorie	Beschreibung
Netzwerke	Verfügt über den Namen der verwendeten Netzwerkkonfiguration, die Art der Adressierung sowie die Netzwerkadressen und VLANs, die dem Firmen- und Gastnetzwerk zugewiesen sind.
Dienste	Verfügt über eine Zusammenfassung der Dienste, die vom VMware SD-WAN-System bereitgestellt werden.

Nachdem alle Einstellungen für die Registerkarten „Profilgerät“ (Profile Device), „Unternehmensrichtlinie“ (Business Policy) und „Firewall“ eingegeben wurden, sollten im Bildschirm **Profilübersicht (Profile Overview)** die von Ihnen vorgenommenen Konfigurationen wiedergegeben werden.

Migration von Netzwerk zu Segment

In der Version 3.2 wurde die Funktion zur Profilmigration eingeführt, um den Workflow zu vereinfachen, mit dem ein Upgrade von Edges von netzwerkbasierten Profilen auf segmentbasierte Profile durchgeführt wird. Dieses Dokument enthält den Workflow und Details zum Upgrade eines 2.X-Edge mit einem netzwerkbasierten Profil auf Version 3.X mit einem segmentbasierten Profil.

Voraussetzungen für das Edge-Upgrade von 2.X auf 3.X

Zum Aktualisieren von Version 2.X auf 3.X sind die folgenden Voraussetzungen für den Edge erforderlich:

- Ein Upgrade von den Versionen 2.4 und 2.5 auf 3.X wird unterstützt.
- Stellen Sie sicher, dass der SD-WAN Orchestrator und das SD-WAN Gateway dieselbe oder eine höhere Version als der Edge aufweisen.

Empfohlene Vorgehensweisen für das Upgrade von Edges als Hub und Spoke

Gehen Sie bei der Durchführung von Upgrades für Edges, die in Hub- und Spoke-Konfigurationen eingesetzt werden, wie folgt vor:

- Die als Hub konfigurierten Edges sollten auf 3.X aktualisiert werden, bevor die als Spokes konfigurierten Edges aktualisiert werden.
- Eine Tunnelbildung findet nicht statt, wenn sich der Hub in einem 3.X-basierten Profil befindet und alle Spokes in einem 2.X-basierten Profil ausgeführt werden.
- Um die oben erwähnte Einschränkung zu überwinden, sollte jedes Spoke-Profil mindestens einen Spoke haben, der im 3.2.1-basierten Profil ausgeführt wird.

Empfohlene Vorgehensweisen für das Upgrade von Edges mit HA

Es gibt keine Beschränkungen für das Upgrade von Edges, die mit HA konfiguriert sind. Normale Softwareschritte sind anwendbar.

Migrieren von Netzwerk zu Segment

Dieser Abschnitt beschreibt die Migration von Netzwerk zu Segment.

Bevor Sie beginnen

- Stellen Sie vor dem Aktualisieren eines Edge sicher, dass der SD-WAN Orchestrator und das SD-WAN Gateway dieselbe Version oder eine höhere Version als der Edge aufweisen.

  Hinweis Da 3.X Edges nur segmentbasierte Profile erkennen, wird das 3.2-Image-Update nur dann an den Edge übertragen, wenn dem Edge ein segmentiertes Profil zugewiesen ist. Sobald einem Edge ein segmentbasiertes Profil zugewiesen wurde, kann es einem netzwerkbasierten Profil nicht neu zugeordnet werden. Der Übergang von einem netzwerkbasierten Profil zu einem segmentbasierten Profil wird unterstützt, der Übergang von einem segmentbasierten Profil zu einem netzwerkbasierten Profil jedoch nicht.

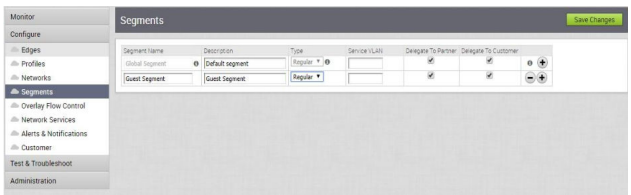
- Stellen Sie sicher, dass die Segmentierung aktiviert ist, bevor Sie ein Profil migrieren.

  Hinweis Standardmäßig ist die Segmentierung aktiviert.

Schritt 1: Erstellen eines nicht globalen Segments für die Zuteilung eines Gastnetzwerks

Da Gastnetzwerke standardmäßig in einem netzwerkbasierten Profil erstellt werden, müssen Sie ein nicht globales Segment erstellen, um die Gastnetzwerke während der Migration einem eigenen Segment zuordnen zu können.

1 Navigieren Sie in SD-WAN Orchestrator zu **Konfigurieren (Configure) > Segmente (Segments)**. Der Bildschirm **Segmente (Segments)** wird angezeigt. Beachten Sie, dass das globale Segment nicht gelöscht werden kann.



2 Klicken Sie auf das Symbol „Hinzufügen“ (Add) ⊕, um ein neues Segment zu erstellen.

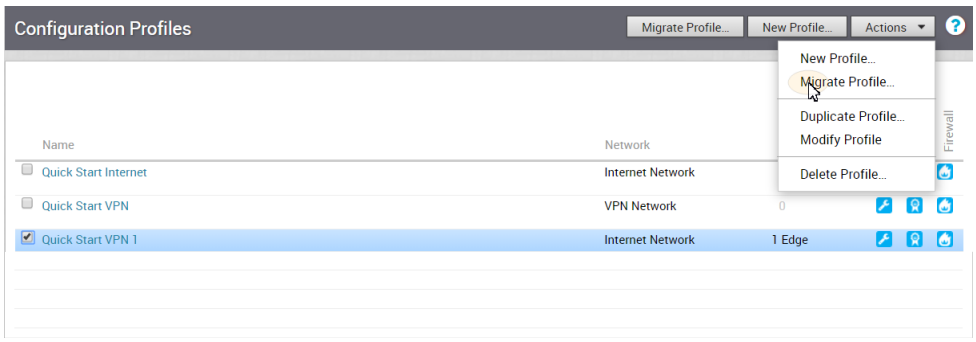
3 Klicken Sie auf **Änderungen speichern (Save Changes)**.

Schritt 2: Erstellen eines migrierten Profils aus einem Netzwerkprofil

1 Gehen Sie im Navigationsbereich von SD-WAN Orchestrator zu **Konfigurieren (Configure) > Profile (Profiles)**.

2 Wählen Sie ein netzwerkbasiertes Profil aus, indem Sie das Kontrollkästchen neben dem Namen des Konfigurationsprofils aktivieren.

3 Wählen Sie im Dropdown-Menü **Aktionen (Actions)** die Option **Profil migrieren (Migrate Profile)** aus.



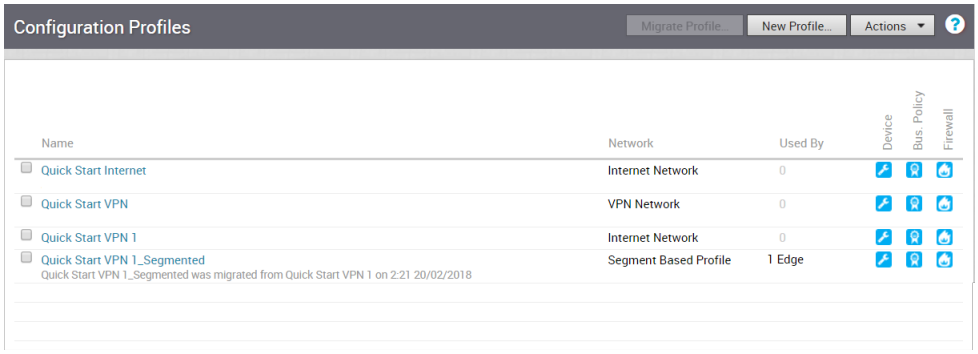
4 Geben Sie im Dialogfeld **Profil migrieren (Migrate Profile)** einen Namen und eine Beschreibung für das Profil ein.

5 Wählen Sie das Segment aus, dem das Gastnetzwerk zugeordnet werden soll (siehe Schritt 4).

Die Konfiguration des Unternehmenssegments wird zum globalen Segment migriert.

6 Klicken Sie auf die Schaltfläche **Erstellen (Create)**.

Ein neues segmentbasiertes Profil wird mit denselben Einstellungen im globalen Segment wie das alte netzwerkbasierte Profil erstellt. Siehe Abbildung unten. Beachten Sie, dass diesem Profil keine Edges zugewiesen sind.



Schritt 3: Zuweisen eines migrierten Profils zu Edges (siehe WICHTIGER HINWEIS unten)

Bei diesem Schritt werden keine Konfigurationsaktualisierungen an den Edge übertragen, während das vom Edge gemeldete Software-Image < 3.0 ist. Die Edges in diesem Zustand weisen im Wesentlichen eine „eingefrorene Konfiguration“ auf, bis ein 3.X-Image für sie bereitgestellt wird.

So weisen Sie einem netzwerkbasierten Edge ein segmentbasiertes Profil zu:

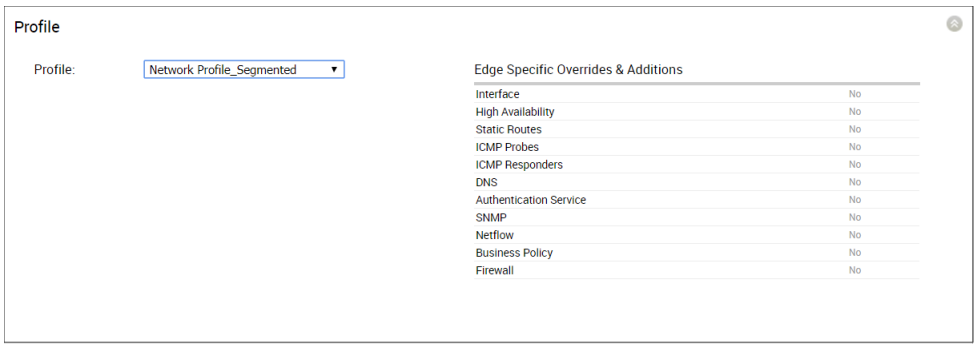
1 Navigieren Sie zu **Konfigurieren (Configure) > Edges** im Navigationsbereich des SD-WAN Orchestrator.

2 Wählen Sie im Bildschirm **Edges** den Edge aus, dem Sie ein Segmentprofil zuweisen möchten.

3 Navigieren Sie auf der Registerkarte **Edge-Übersicht (Edge Overview)** zum Bereich **Profil (Profile)**.

4 Wählen Sie im Dropdown-Menü **Profil (Profile)** ein **Segmentbasiertes Profil (Segment Based Profile)** aus.

Das segmentbasierte Profil wird erst angewendet, nachdem das Upgrade des Edge auf 3.2.X erfolgt ist.



Hinweis Es gibt zwei zusätzliche Schritte, um ein Profil zu migrieren: „Erstellen eines neuen Operator-Profils mit einem 3.2-Edge-Image“ und „Zuweisen des segmentbasierten Operator-Profils zu den Edges“. Die Enterprise-Admin-Benutzer auf allen Ebenen haben keinen Zugriff auf diese zusätzlichen Schritte und müssen sich an ihren Operator wenden. Ihr Operator muss ein neues Operator-Profil mit einem 3.X-Image erstellen und das Operator-Profil für die Nutzung durch das Unternehmen zuweisen. Nach dem Zuweisen des 3.X-basierten Operator-Profils und des segmentierten Profils erhält der Edge ein Software-Image-Update. Weitere Informationen erhalten Sie bei Ihrem Operator.

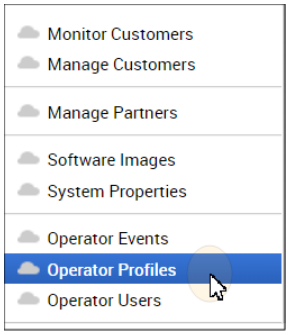
Hinweis Der nächste Schritt, „Erstellen eines neuen Operator-Profils mit einem 3.2-Edge-Image“ ist ein Schritt, der nur auf Operator-Ebene ausgeführt wird und der abgeschlossen sein muss, bevor ein Profil migriert werden kann. Partner haben keinen Zugriff auf die Funktionen für diesen Schritt und müssen sich an ihre Operatoren wenden.

Schritt 4: Erstellen eines neuen Operator-Profils mit einem 3.2-Edge-Image (Schritt nur auf Operator-Ebene)

Operatoren müssen ein neues Operator-Profil mit einem 3.2-Edge-Image erstellen, bevor ein Profil migriert werden kann. Benutzer auf Enterprise- und Partner-Ebene haben keinen Zugriff auf die Funktionen in diesem Schritt.

Schritt 5 wird nur auf Operator-Ebene durchgeführt. Ihr Operator muss ein neues Operator-Profil mit einem 3.2-Edge-Image erstellen.

1 Wählen Sie in SD-WAN Orchestrator die Option **Operator-Profile (Operator Profiles)** aus. Siehe Abbildung unten.



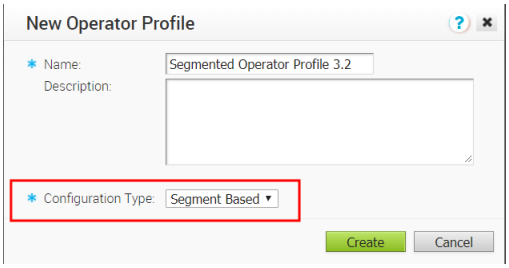
2 Klicken Sie im Bildschirm **Operator-Profil (Operator Profile)** auf die Schaltfläche **Neues Profil (New Profile)**.

3 Im Dialogfeld **Neues Operator-Profil (New Operator Profile)**:

   a Geben Sie einen Dateinamen und eine Beschreibung für das Profil ein.

   b Wählen Sie im Dropdown-Menü **Konfigurationstyp (Configuration Type)** die Option **Segmentbasiert (Segment Based)** aus.

   c Klicken Sie auf die Schaltfläche **Erstellen (Create)**.



4 Navigieren Sie im neu erstellten Bildschirm **Operator-Profil (Operator Profile)** zum Bereich **Softwareversion (Software Version)**.

5 Wählen Sie im Bereich **Softwareversion (Software Version)** im Dropdown-Menü **Version** eine Softwareversion aus. (Siehe Abbildung unten.)

6 Klicken Sie auf die Schaltfläche **Änderungen speichern (Save Changes)** oben im Bildschirm SD-WAN Orchestrator.

Schritt 6: Zuweisen des segmentbasierten Operator-Profils zu den Edges

Diesem Schritt wurde für die Softwareversion 3.3.0 ein wichtiger Hinweis hinzugefügt (siehe Hinweis unten).

Hinweis Operatoren und Partner können Software-Images zuweisen, Enterprise-Administratoren auf allen Ebenen haben jedoch keinen Zugriff auf diese Funktion.

Der Edge mit dem segmentierten Profil erhält ein Software-Image-Update über das Operator-Profil. Dies kann entweder durch das Wechseln des Operator-Profils für den Kunden oder durch die Zuweisung eines neuen Operator-Profils zu ausgewählten Edges erfolgen. In den unten aufgeführten Schritten wird beschrieben, wie Sie einem ausgewählten Edge ein neues Operator-Profil zuweisen.

Hinweis Es wird empfohlen, dass Sie zuerst die Profilzuweisung zu einem Edge durchführen und überprüfen, ob der Edge ordnungsgemäß funktioniert, bevor Sie mit den anderen Edges fortfahren. Der erste Edge, dem Sie ein Profil zuweisen, wird als Hub klassifiziert (da Hubs vor Spokes migriert werden müssen).

So weisen Sie ein neues Operator-Profil zu:

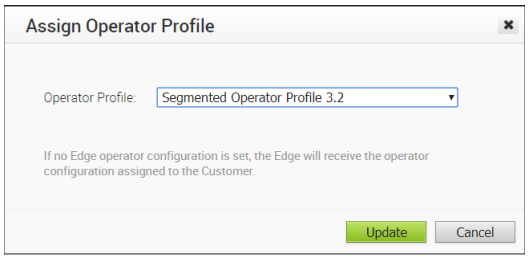
1 Gehen Sie im Navigationsbereich von SD-WAN Orchestrator zu **Konfigurieren (Configure) > Edges**.

2 Wählen Sie im Bildschirm **Edges** die Edges aus, denen Sie ein Operator-Profil zuweisen möchten.

3 Wählen Sie im Dropdown-Menü **Aktionen (Actions)** die Option **Operator-Profil zuweisen (Assign Operator Profile)** oder **Software-Image zuweisen (Assign Software Image)** aus. (HINWEIS: Nur Operator-Superusern wird die Option **Operator-Profil zuweisen (Assign Operator Profile)** im Dropdown-Menü **Aktionen (Actions)** angezeigt. Allen anderen Benutzern mit Zugriff auf diese Funktion wird im Dropdown-Menü **Aktionen (Actions)** die Option **Software-Image zuweisen (Assign Software Image)** angezeigt.)

4 Wählen Sie im entsprechenden Dialogfeld (Dialogfeld **Operator-Profil zuweisen (Assign Operator Profile)** oder Dialogfeld **Software-Image zuweisen (Assign Software Image)**) das segmentbasierte Operator-Profil aus, das in Schritt 3 erstellt wurde. (**HINWEIS:** Weisen Sie das Operator-Profil bei Bedarf einem Kunden oder Partner zu.)

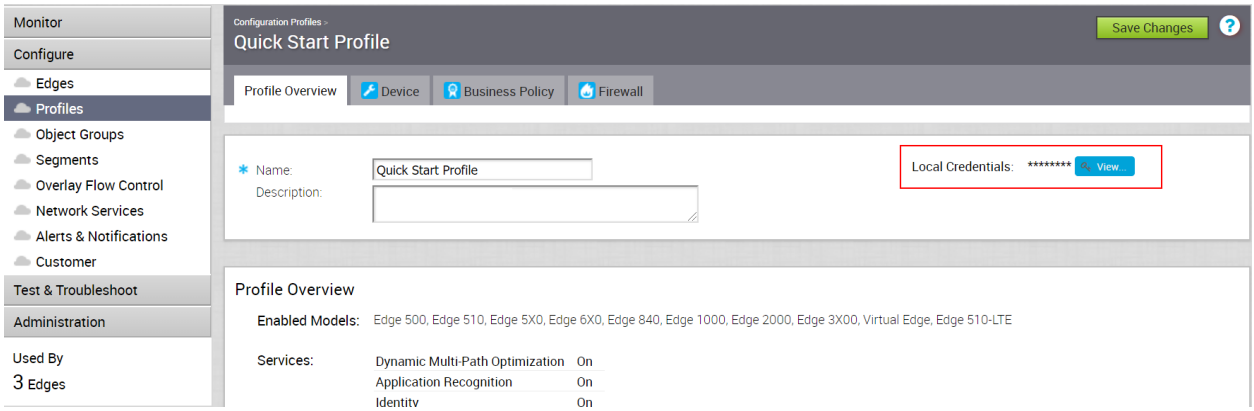
5 Klicken Sie auf die Schaltfläche **Aktualisieren (Update)**.



Nach diesem Vorgang erhalten Edges das Software-Image-Update 3.2. Nachdem der Image-Update-Prozess abgeschlossen ist, beginnen die Edges mit dem SD-WAN Orchestrator zu kommunizieren.

Konfigurieren lokaler Anmeldedaten

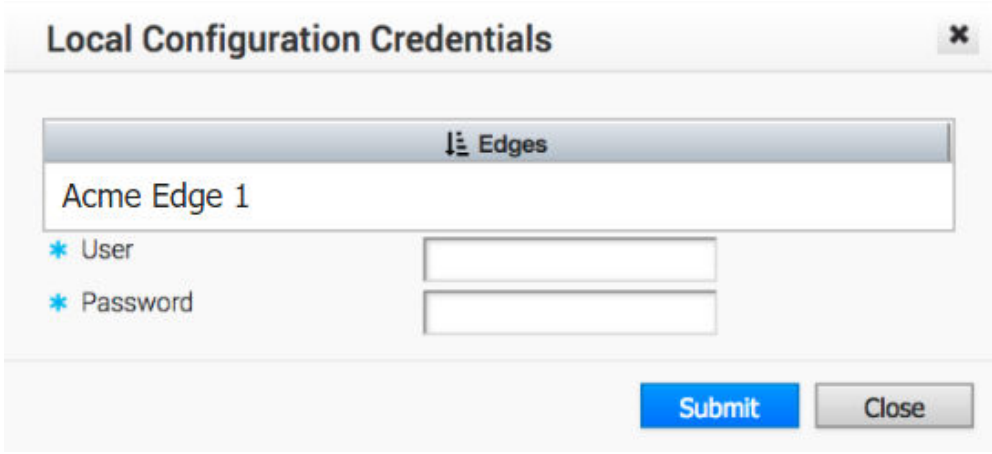
Sie können die lokalen Anmeldedaten auf Profilebene über die Registerkarte **Konfigurieren (Configure) > Profil (Profile) > Profilübersicht (Profile Overview)** ändern. Nach dem Aktualisieren der Anmeldedaten werden diese an alle Edges gesendet, die das Profil als Edge-Aktion verwenden.



Hinzufügen von Anmeldedaten

In diesem Abschnitt wird beschrieben, wie Sie Anmeldedaten hinzufügen.

Klicken Sie auf die Schaltfläche **Ansicht (View)**, um das Dialogfeld **Lokale Konfigurationsanmeldedaten (Local Configuration Credentials)** zu öffnen. Nehmen Sie die Eingaben unter **Benutzer (User)** und **Kennwort (Password)** vor und klicken Sie auf die Schaltfläche **Übermitteln (Submit)**.


Local Configuration Credentials
Edges
Acme Edge 1
* User
* Password
Submit
Close

Konfigurieren eines Profilgeräts 10

In diesem Abschnitt wird beschrieben, wie Sie ein Profilgerät konfigurieren.

Hinweis Wenn Sie mit einer Benutzer-ID mit Kundensupport-Berechtigungen angemeldet sind, können Sie nur SD-WAN Orchestrator-Objekte anzeigen. Sie werden nicht in der Lage sein, neue Objekte zu erstellen oder bestehende zu konfigurieren/aktualisieren.

VMware SD-WAN stellt Geräteeinstellungen mithilfe der Registerkarte **Gerät (Device)** (**Konfigurieren (Configure) > Profile (Profiles) > Registerkarte „Gerät“ (Device Tab)**) in einem Profil bereit. Die Registerkarte **Geräteeinstellungen (Device Settings)** wird verwendet, um Segmente zuzuweisen, VLANs zu erstellen, Schnittstellen zu konfigurieren, DNS-Einstellungen zu konfigurieren und Authentifizierungseinstellungen zu konfigurieren. Weitere Informationen zur Segmentierung finden Sie unter Kapitel 7 Konfigurieren von Segmenten.

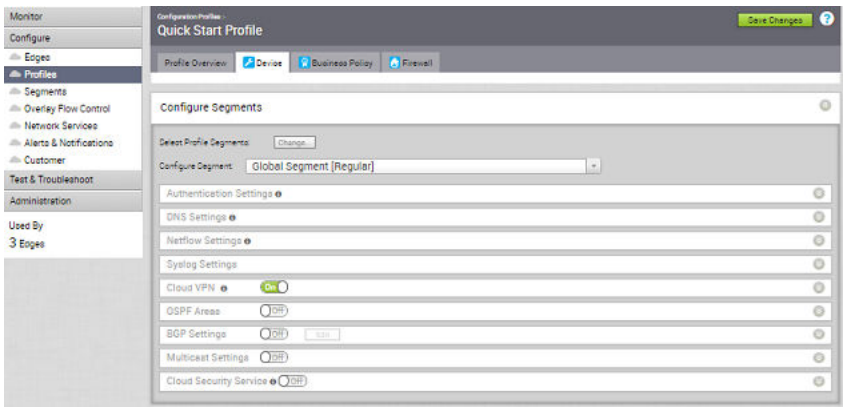
Dieses Kapitel enthält die folgenden Themen:

Konfigurieren eines Geräts

Die Gerätekonfiguration ermöglicht es Ihnen, Segmente einem Profil zuzuordnen und Schnittstellen so zu konfigurieren, dass sie mit einem Profil verknüpft werden.

Für segmentierfähige Profile gibt es zwei Abschnitte auf der Benutzeroberfläche:

Konfigurationstyp	Beschreibung
Segmentierfähige Konfigurationen	Bereich **Segmente konfigurieren (Configure Segments)** auf der Registerkarte **Gerät (Device)**. Kunden können das Segment im Dropdown-Menü wählen und dann das Segment auswählen. Im Anschluss daran wird die Konfiguration für dieses Segment im Bereich **Segmente konfigurieren (Configure Segments)** angezeigt.
Häufige Konfigurationen	Der untere Teil der Registerkarte **Gerät (Device)**. Funktionen und Konfigurationen, die für mehrere Segmente gelten, darunter VLAN-Konfigurationen, Geräteeinstellungen, WLAN und QoS mit Mehrfachquelle.



Sie können die folgenden Schritte für die Gerätekonfiguration ausführen:

Segmentierfähige Konfigurationen

- Authentifizierungseinstellungen (Authentication Settings)
- DNS-Einstellungen (DNS Settings)
- NetFlow-Einstellungen (Netflow Settings)
- Syslog-Einstellungen (Syslog Settings)
- Cloud-VPN (Cloud VPN)
- OSPF-Bereiche (OSPF Areas)
- BGP-Einstellungen (BGP Settings)
- Multicast-Einstellungen (Multicast Settings)
- Cloud-Sicherheitsdienst (Cloud Security Service)

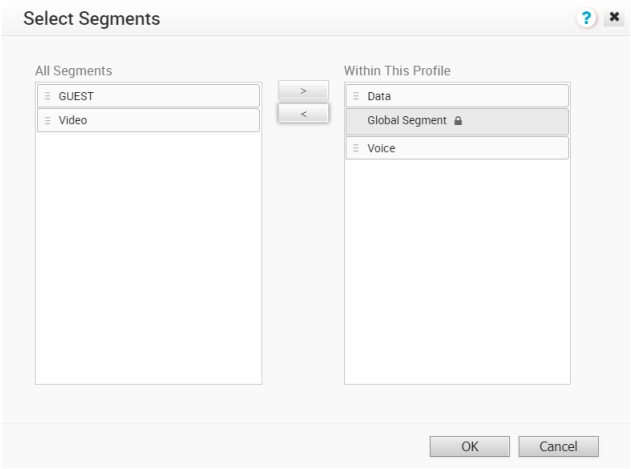
Häufige Konfigurationen:

- VLAN
- Geräteeinstellungen (Device Settings)
- WLAN-Funkeinstellungen (Wi-Fi Radio Settings)
- QoS mit Mehrfachquelle (Multi-Source QoS)
- SNMP-Einstellungen (SNMP Settings)
- NTP-Server (NTP Servers)
- Sichtbarkeitsmodus (Visibility Mode)

Zuweisen von Segmenten in einem Profil

Nachdem Sie ein Profil erstellt haben, können Sie Profilsegmente auswählen, indem Sie auf die Schaltfläche **Ändern (Change)** im Fenster **Segmente konfigurieren (Configure Segments)** klicken.

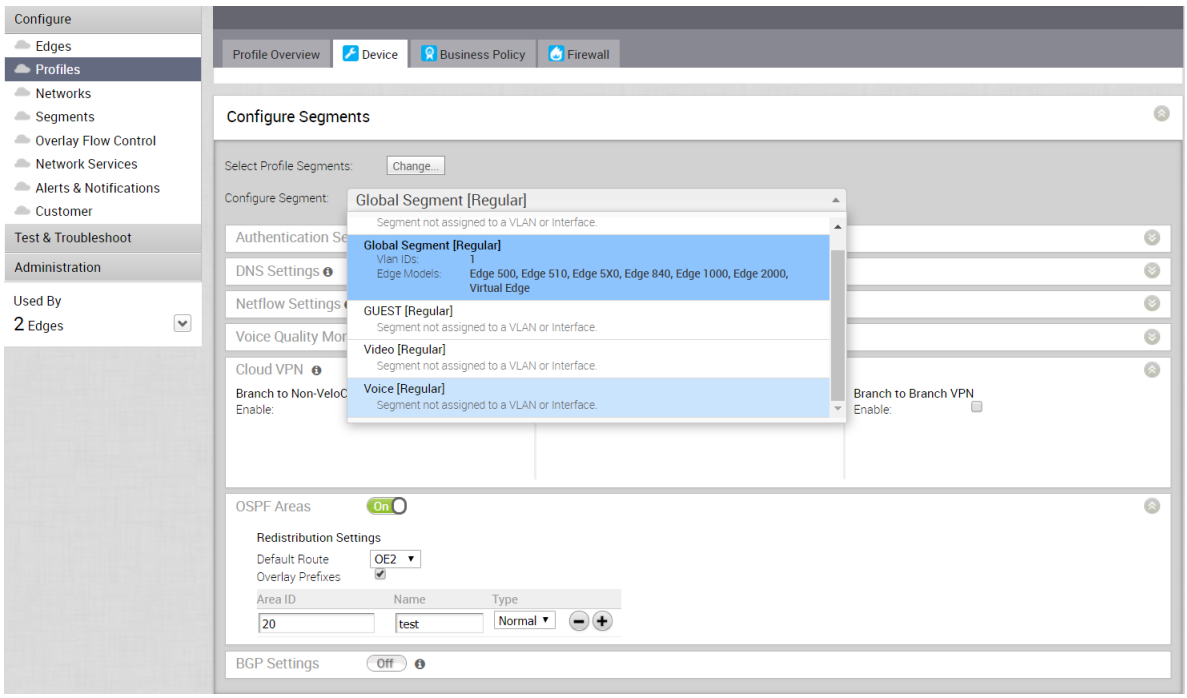
Wenn Sie auf die Schaltfläche**Ändern (Change)** klicken, wird das Dialogfeld **Segmente auswählen (Select Segments)** geöffnet.



In diesem Dialogfeld können Sie die Segmente auswählen, die Sie in Ihr Profil aufnehmen möchten. Segmente mit einem Schlosssymbol daneben zeigen an, dass das Segment innerhalb eines Profils verwendet wird und nicht entfernt werden kann. Die zur Verwendung verfügbaren Segmente werden auf der linken Seite des Dialogfelds unter **Alle Segmente (All Segments)** angezeigt.

Nachdem Sie ein Segment ausgewählt haben, können Sie Ihr Segment über das Dropdown-Menü **Segment konfigurieren (Configure Segment)** konfigurieren. Alle für die Konfiguration verfügbaren Segmente werden im Dropdown-Menü **Segment konfigurieren (Configure Segment)** aufgelistet. Wenn ein Segment einem VLAN oder einer Schnittstelle zugeordnet ist, zeigt es die VLAN-ID und die damit verbundenen Edge-Modelle an.

Wenn Sie ein zu konfigurierendes Segment aus dem Dropdown-Menü **Segment konfigurieren (Configure Segment)** auswählen, werden je nach den Optionen des Segments die mit diesem Segment verbundenen Einstellungen im Bereich **Segmente konfigurieren (Configure Segments)** angezeigt.



Konfigurieren von Authentifizierungseinstellungen

Mit den **Einstellungen für die Geräteauthentifizierung (Device Authentication Settings)** können Sie angeben, welche Netzwerkdienste für den DNS-Server verwendet werden sollen.

Konfigurieren von DNS-Einstellungen

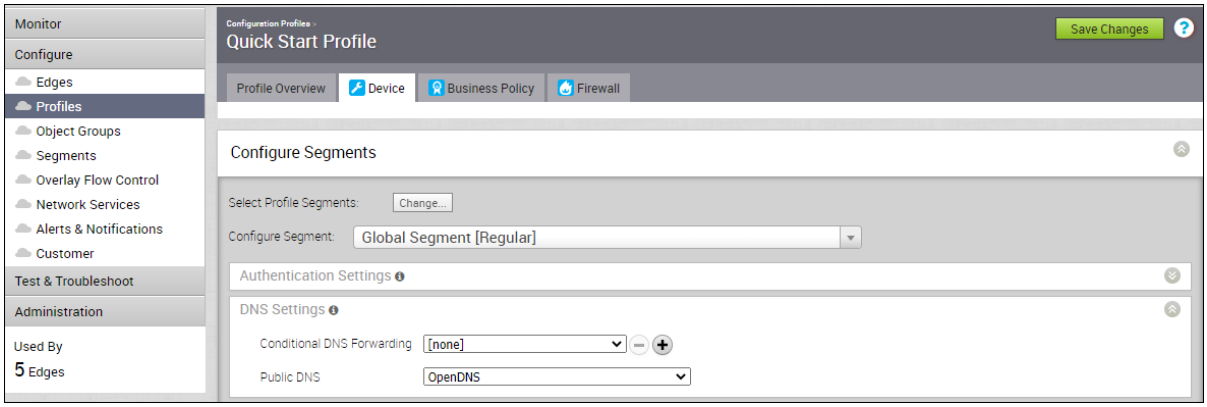
Die **DNS-Einstellungen (DNS Settings)** können verwendet werden, um die bedingte DNS-Weiterleitung über einen privaten DNS-Dienst zu konfigurieren und einen öffentlichen DNS-Dienst anzugeben, der für Abfragezwecke verwendet werden soll.

So konfigurieren Sie die DNS-Einstellungen:

1 Klicken Sie im Unternehmensportal auf **Konfigurieren (Configure) > Profile (Profiles)**.

2 Klicken Sie auf das Gerätesymbol neben einem Profil oder klicken Sie auf den Link zum Profil und dann auf die Registerkarte **Gerät (Device)**.

3 Konfigurieren Sie auf der Registerkarte **Gerät (Device)** im Abschnitt **DNS-Einstellungen (DNS Settings)** die folgenden Einstellungen:



- **Bedingte DNS-Weiterleitung (Conditional DNS Forwarding)**: Wählen Sie einen privaten DNS-Dienst in der Dropdown-Liste aus, um die mit dem Domänennamen verbundenen DNS-Anforderungen weiterzuleiten. Sie können auch auf **Neuer privater DNS-Dienst (New Private DNS Service)** klicken, um einen neuen privaten DNS-Dienst zu erstellen.
- **Öffentlicher DNS (Public DNS)**: Wählen Sie einen öffentlichen DNS-Dienst aus der Dropdown-Liste aus, der für die Abfrage der Domänennamen verwendet werden soll. Sie können auch auf **Neuer DNS-Dienst (New DNS Service)** klicken, um einen neuen öffentlichen DNS-Dienst zu erstellen.

Weitere Informationen zum Erstellen eines neuen DNS-Diensts finden Sie unter Konfigurieren von DNS-Diensten.

4 Klicken Sie auf der Registerkarte **Gerät (Device)** auf **Änderungen speichern (Save Changes)**.

Hinweis Die globale Segmentkonfiguration für DNS gilt für alle vom Kunden erstellten Segmente. Die Quell-IP ist die Verwaltungs-IP-Adresse, die im Abschnitt **VLAN konfigurieren (Configure VLAN)** konfiguriert ist. Weitere Informationen finden Sie unter Konfigurieren von VLAN für Profile.

Konfigurieren von Netflow-Einstellungen auf der Profilebene

Als Unternehmensadministrator können Sie die Netflow-Einstellungen auf der Profilebene konfigurieren.

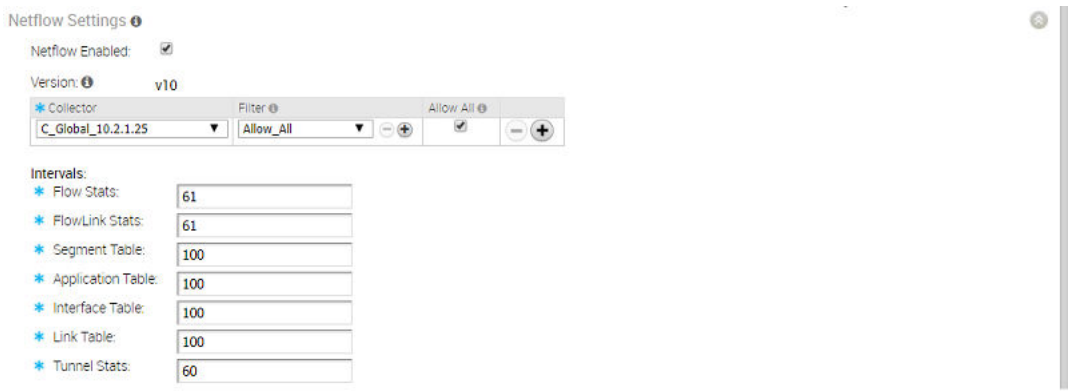
Verfahren

1 Navigieren Sie in SD-WAN Orchestrator zu **Konfigurieren (Configure)** > **Profile (Profiles)**.

Die Seite **Konfigurationsprofile (Configuration Profiles)** wird angezeigt.

2 Wählen Sie ein Profil aus, für das Sie NetFlow-Einstellungen konfigurieren möchten, und klicken Sie auf das Symbol in der Spalte **Gerät (Device)**.

Die Seite „Geräteeinstellung (Device Setting)“ für das ausgewählte Profil wird angezeigt.



3 Wählen Sie im Dropdown-Menü **Segment konfigurieren (Configure Segment)** ein Profilsegment aus, um die NetFlow-Einstellungen zu konfigurieren.

4 Navigieren Sie zum Bereich **Netflow-Einstellungen (Netflow Settings)** und konfigurieren Sie die folgenden Details.

a Aktivieren Sie das Kontrollkästchen **Netflow aktiviert (Netflow Enabled)**.

SD-WAN Orchestrator unterstützt die IPFIX (IP Flow Information Export)-Protokoll Version 10.

b Wählen Sie im Dropdown-Menü **Collector** einen vorhandenen NetFlow-Collector aus, um IPFIX-Informationen direkt aus SD-WAN Edges zu exportieren, oder klicken Sie auf **Neuer Collector (New Collector)**, um einen neuen NetFlow-Collector zu konfigurieren.

Weitere Informationen zum Hinzufügen einer neuen Collector-Instanz finden Sie unter Konfigurieren von Netflow-Einstellungen.

Hinweis Sie können maximal zwei Collector-Instanzen pro Segment und acht Collector-Instanzen pro Profil konfigurieren, indem Sie auf die Schaltfläche **+** klicken. Wenn die Anzahl der konfigurierten Collector-Instanzen den maximal zulässigen Grenzwert erreicht, wird die Schaltfläche **+** deaktiviert.

c Wählen Sie im Dropdown-Menü **Filter** einen vorhandenen NetFlow-Filter für die Datenverkehrsströme aus SD-WAN Edges aus oder klicken Sie auf **Neuer Filter (New Filter)**, um einen neuen NetFlow-Filter zu konfigurieren.

Weitere Informationen zum Hinzufügen eines neuen Filters finden Sie unter Konfigurieren von Netflow-Einstellungen.

Hinweis Sie können maximal 16 Filter pro Collector konfigurieren, indem Sie auf die Schaltfläche **+** klicken. Die Filterregel „Alle zulassen (Allow All)“ wird jedoch implizit am Ende der definierten Filterliste pro Collector hinzugefügt.

d Aktivieren Sie das Kontrollkästchen **Alle zulassen (Allow All)** für einen Collector, um alle Segmentflüsse zu diesem Collector zuzulasssen.

e Konfigurieren Sie unter **Intervalle (Intervals)** die folgenden Netflow-Exportintervalle:

- **Flow-Statistik (Flow Stats)**: Exportintervall für die Flow-Statistikvorlage, die die Flow-Statistik an den Collector exportiert. Standardmäßig werden die NetFlow-Datensätze dieser Vorlage alle 60 Sekunden exportiert. Der zulässige Exportintervallbereich liegt zwischen 60 Sekunden und 300 Sekunden.
- **FlowLink-Statistik (FlowLink Stats)**: Exportintervall für die FlowLink-Statistik, die die Flussstatistik per Verknüpfung an den Collector exportiert. Standardmäßig werden die NetFlow-Datensätze dieser Vorlage alle 60 Sekunden exportiert. Der zulässige Exportintervallbereich liegt zwischen 60 Sekunden und 300 Sekunden.
- **VRF-Tabelle (VRF Table)**: Exportintervall für VRF-Optionsvorlage, die segmentbezogene Informationen an den Collector exportiert. Das Standardexportintervall beträgt 300 Sekunden. Der zulässige Exportintervallbereich liegt zwischen 60 Sekunden und 300 Sekunden.
- **Anwendungstabelle (Application Table)**: Exportintervall für die Anwendungsoptionsvorlage, die Anwendungsinformationen an den Collector exportiert. Das Standardexportintervall beträgt 300 Sekunden. Der zulässige Exportintervallbereich liegt zwischen 60 Sekunden und 300 Sekunden.
- **Schnittstellentabelle (Interface Table)**: Exportintervall für die Schnittstellenoptionsvorlage, die Schnittstelleninformationen an den Collector exportiert. Das Standardexportintervall beträgt 300 Sekunden. Der zulässige Exportintervallbereich liegt zwischen 60 Sekunden und 300 Sekunden.
- **Link-Tabelle (Link Table)**: Exportintervall für die Link-Optionsvorlage, die die Link-Informationen an den Collector exportiert. Das Standardexportintervall beträgt 300 Sekunden. Der zulässige Exportintervallbereich liegt zwischen 60 Sekunden und 300 Sekunden.
- **Tunnelstatistik (Tunnel Stats)**: Exportintervall für die Tunnelstatistikvorlage. Standardmäßig wird die Statistik der aktiven Tunnel im Edge alle 60 Sekunden exportiert. Der zulässige Exportintervallbereich liegt zwischen 60 Sekunden und 300 Sekunden.

Hinweis In einem Unternehmen können Sie die Netflow-Intervalle für jede Vorlage nur auf dem globalen Segment konfigurieren. Das konfigurierte Netflow-Exportintervall gilt für alle Collector-Instanzen aller Segmente auf einem Edge.

5 Klicken Sie auf **Änderungen speichern (Save Changes)**.

Konfigurieren von Syslog-Einstellungen auf der Profilebene

In einem Unternehmensnetzwerk unterstützt SD-WAN Orchestrator die Erfassung von SD-WAN Orchestrator-gebundenen Ereignissen und Firewallprotokollen, die vom Unternehmens-SD-WAN

Edges stammen, in einer oder mehreren zentralen Remote-Syslog-Collector-Instanzen (Server) im nativen Syslog-Format. Damit der Syslog-Collector SD-WAN Orchestrator-gebundene Ereignisse und Firewallprotokolle von den konfigurierten Edges in einem Unternehmen empfangen kann, konfigurieren Sie auf der Profilebene die Details des Syslog-Collectors pro Segment auf der SD-WAN Orchestrator-Instanz, indem Sie die Schritte in diesem Verfahren ausführen.

Voraussetzungen

- Stellen Sie sicher, dass Cloud-Virtual Private Network (Zweigstelle-zu-Zweigstelle-VPN-Einstellungen) für den SD-WAN Edge konfiguriert ist (von dem die SD-WAN Orchestrator-gebundenen Ereignisse stammen), um einen Pfad zwischen dem SD-WAN Edge und den Syslog-Collector-Instanzen einzurichten. Weitere Informationen finden Sie unter Konfigurieren von Cloud-VPN.

Verfahren

1 Navigieren Sie in SD-WAN Orchestrator zu **Konfigurieren (Configure)** > **Profile (Profiles)**.

   Die Seite **Konfigurationsprofile (Configuration Profiles)** wird angezeigt.

2 Wählen Sie ein Profil aus, für das Sie die Syslog-Einstellungen konfigurieren möchten, und klicken Sie auf das Symbol unter der Spalte **Gerät (Device)**.

   Die Seite „Geräteeinstellungen (Device Settings)“ wird für das ausgewählte Profil angezeigt.

3 Wählen Sie im Dropdown-Menü **Segment konfigurieren (Configure Segment)** ein Profilsegment aus, um die Syslog-Einstellungen zu konfigurieren. Standardmäßig ist **Globales Segment [Normal] (Global Segment [Regular])** ausgewählt.

4 Navigieren Sie zum Bereich **Syslog-Einstellungen (Syslog Settings)** und konfigurieren Sie die folgenden Details.

   a Wählen Sie im Dropdown-Menü **Anlagencode (Facility Code)** einen Syslog-Standardwert aus, der festlegt, wie Ihr Syslog-Server das Anlagenfeld verwendet, um Meldungen für alle Ereignisse aus SD-WAN Edges zu verwalten. Die zulässigen Werte reichen von **local0** bis **local7**.

   Hinweis Das Feld **Anlagencode (Facility Code)** ist nur für **Globales Segment (Global Segment)** konfigurierbar, egal, ob die Syslog-Einstellungen für das Profil aktiviert sind oder nicht. Die anderen Segmente erben den Wert des Anlagencodes aus dem globalen Segment.

   b Aktivieren Sie das Kontrollkästchen **Syslog aktiviert (Syslog Enabled)**.

   c Geben Sie im Textfeld **IP** die Ziel-IP-Adresse des Syslog-Collectors ein.

   d Wählen Sie im Dropdown-Menü **Protokoll (Protocol)** entweder **TCP** oder **UDP** als Syslog-Protokoll aus.

   e Geben Sie im Textfeld **Port** die Portnummer des Syslog-Collectors ein. Der Standardwert ist 514.

f Da Edge-Schnittstellen auf der Profilebene nicht verfügbar sind, wird das Feld **Quellschnittstelle (Source Interface)** auf **Automatisch (Auto)** festgelegt. Der Edge wählt automatisch eine Schnittstelle aus, bei der das Feld „Ankündigen (Advertise)“ als Quellschnittstelle eingestellt ist.

g Wählen Sie im Dropdown-Menü **Rollen (Roles)** eine der folgenden Optionen aus:

- **EDGE-EREIGNIS (EDGE EVENT)**
- **FIREWALL-EREIGNIS (FIREWALL EVENT)**
- **EDGE- UND FIREWALL-EREIGNIS (EDGE AND FIREWALL EVENT)**

h Wählen Sie im Dropdown-Menü **Syslog-Ebene (Syslog Level)** den Syslog-Schweregrad aus, der konfiguriert werden muss. Wenn beispielsweise **KRITISCH (CRITICAL)** konfiguriert ist, sendet der SD-WAN Edge alle Ereignisse, die entweder als kritisch oder als Warnung oder Notfall festgelegt sind.

Hinweis Firewallereignisprotokolle werden standardmäßig mit dem Syslog-Schweregrad **INFO** weitergeleitet.

Zulässige Syslog-Schweregrade:

- **NOTFALL (EMERGENCY)**
- **ALARM (ALERT)**
- **KRITISCH (CRITICAL)**
- **FEHLER (ERROR)**
- **WARNUNG (WARNING)**
- **HINWEIS (NOTICE)**
- **INFO**
- **DEBUGGEN (DEBUG)**

i Geben Sie optional im Textfeld **Tag** ein Tag für das Syslog ein. Das Syslog-Tag kann verwendet werden, um die verschiedenen Ereignistypen auf dem Syslog-Collector zu differenzieren. Die maximal zulässige Zeichenlänge beträgt 32 (getrennt durch einen Punkt).

j Aktivieren Sie bei der Konfiguration eines Syslog-Collectors mit der Rolle **FIREWALL-EREIGNIS (FIREWALL EVENT)** oder **EDGE- UND FIREWALL-EREIGNIS (EDGE AND FIREWALL EVENT)** das Kontrollkästchen **Alle Segmente (All Segments)**, wenn der Syslog-Collector Firewallprotokolle aus allen Segmenten erhalten soll. Wenn das Kontrollkästchen deaktiviert ist, empfängt der Syslog-Collector nur Firewallprotokolle aus dem Segment, in dem der Collector konfiguriert ist.

Hinweis Wenn die Rolle **EDGE-EREIGNIS (EDGE EVENT)** verwendet wird, empfängt der in einem beliebigen Segment konfigurierte Syslog-Collector standardmäßig Edge-Ereignisprotokolle.

5 Klicken Sie auf die Schaltfläche **+**, um einen weiteren Syslog-Collector hinzuzufügen, oder klicken Sie auf **Änderungen speichern (Save Changes)**. Der Remote-Syslog-Collector ist in SD-WAN Orchestrator konfiguriert.

Hinweis Sie können maximal zwei Syslog-Collectors pro Segment und 10 Syslog-Collectors pro Edge konfigurieren. Wenn die Anzahl der konfigurierten Collector-Instanzen den maximal zulässigen Grenzwert erreicht, wird die Schaltfläche **+** deaktiviert.

Hinweis Basierend auf der ausgewählten Rolle exportiert der Edge die entsprechenden Protokolle mit dem angegebenen Schweregrad auf den Remote-Syslog-Collector. Wenn Sie möchten, dass die von SD-WAN Orchestrator automatisch erstellen lokalen Ereignisse auf dem Syslog-Collector empfangen werden, müssen Sie Syslog auf der SD-WAN Orchestrator-Ebene mithilfe der Systemeinstellungen `log.syslog.backend` und `log.syslog.upload` konfigurieren.

Informationen zum Format einer Syslog-Nachricht für Firewall-Protokolle finden Sie unter Format der Syslog-Meldungen für Firewallprotokolle.

Nächste Schritte

SD-WAN Orchestrator ermöglicht es Ihnen, die Funktion „Syslog-Weiterleitung (Syslog Forwarding)“ im Profil und auf dem Edge zu aktivieren. Aktivieren Sie auf der Seite **Firewall** der Profilkonfiguration die Schaltfläche **Syslog-Weiterleitung (Syslog Forwarding)**, wenn Sie Firewallprotokolle, die vom Unternehmens-SD-WAN Edges stammen, an konfigurierte Syslog-Collector-Instanzen weiterleiten möchten.

Hinweis Standardmäßig ist die Schaltfläche **Syslog-Weiterleitung (Syslog Forwarding)** auf der Seite **Firewall** der Profil- oder Edge-Konfiguration verfügbar und deaktiviert.

Weitere Informationen zu Firewalleinstellungen auf der Profilebene finden Sie unter Konfigurieren der Firewall für Profile.

Format der Syslog-Meldungen für Firewallprotokolle

Beschreibt das Syslog-Meldungsformat für Firewallprotokolle mit einem Beispiel.

Beispiel: IETF-Syslog-Meldungsformat (RFC 3164)

```
<%PRI%>%timegenerated% %HOSTNAME% %syslogtag%%msg
```

Im Folgenden finden Sie eine Syslog-Beispielmeldung.

```
<158>Dec 17 07:21:16 b1-edge1 velocloud.sdwan: VCF Open xR6FveSQT220kZiTmoYJHA SID=12278 SEGMENT=0
IN="IFNAME" PROTO=ICMP SRC=x.x.x.x DST=x.x.x.x DEST_NAME=Internet-via-gateway-3
```

Die Meldung enthält die folgenden Teile:

- Priorität - Anlage * 8 + Schweregrad (local4 & kritisch) - 158
- Datum - 17. Dez
- Uhrzeit - 07:21:16
- Hostname - b1-edge1
- Syslog-Tag - velocloud.sdwan
- Meldung - VCF Open xR6FveSQT220kZiTmoYJHA SID=12278 SEGMENT=0 IN="IFNAME" PROTO=ICMP SRC=x.x.x.x DST=x.x.x.x DEST_NAME=Internet-via-gateway-3

VMware SD-WAN unterstützt die folgenden Firewallprotokollmeldungen:

- Mit aktivierter statusbehafteten Firewall:
  - Öffnen – Die Datenverkehrssitzung wurde gestartet.
  - Schließen – Die Datenverkehrssitzung wurde aufgrund einer Zeitüberschreitung der Sitzung beendet oder die Sitzung wird durch den Orchestrator geleert.
  - Verweigern – Wenn die Sitzung mit der Verweigern-Regel übereinstimmt, wird die Verweigern-Protokollnachricht angezeigt und das Paket wird gelöscht. Im Fall von TCP wird das Zurücksetzen an die Quelle gesendet.
  - Update – Für alle laufenden Sitzungen wird die Update-Protokollnachricht angezeigt, wenn die Firewallregel entweder hinzugefügt oder über Orchestrator geändert wird.
- Bei deaktivierter statusbehafteter Firewall:
  - Zulassen
  - Verweigern

Tabelle 10-1. Felder für Firewallprotokollmeldungen

Feld	Beschreibung
SID	Die eindeutige Identifikationsnummer, die auf jede Sitzung angewendet wird.
SVLAN	Die VLAN-ID des Quellgeräts.
DVLAN	Die VLAN-ID des Zielgeräts.
SEGMENT	Das Segment, zu dem die Sitzung gehört. Der zulässige Bereich liegt zwischen 0 und 255.

Tabelle 10-1. Felder für Firewallprotokollmeldungen (Fortsetzung)

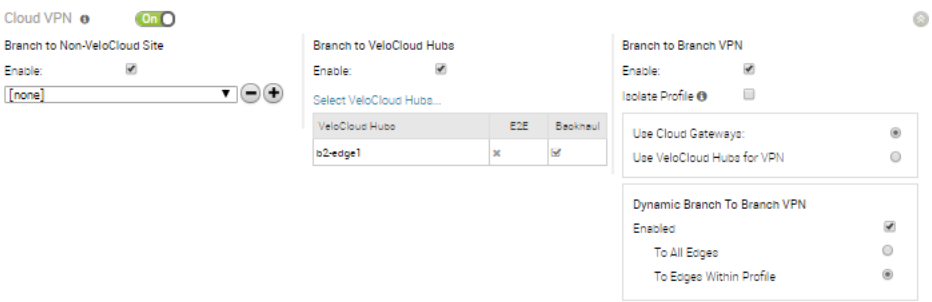
Feld	Beschreibung
IN	Der Schnittstellenname, auf dem das erste Paket der Sitzung empfangen wurde. Im Falle von empfangenen Overlay-Paketen enthält dieses Feld **VPN**. Bei allen anderen Paketen (durch Underlay empfangen) wird in diesem Feld der Name der Schnittstelle im Edge angezeigt.
PROTO	Der Typ des von der Sitzung verwendeten IP-Protokolls. Die möglichen Werte sind TCP, UDP, GRE, ESP und ICMP.
SRC:	Die Quell-IP-Adresse der Sitzung in punktierter Dezimalnotation.
DST	Die Ziel-IP-Adresse der Sitzung in punktierter Dezimalnotation.
SPT	Die Quellportnummer der Sitzung. Dieses Feld ist nur anwendbar, wenn der zugrunde liegende Transport UDP/TCP ist.
DPT	Die Zielportnummer der Sitzung. Dieses Feld ist nur anwendbar, wenn der zugrunde liegende Transport UDP/TCP ist.
DEST_NAME	Der Name des Remote-Endgeräts der Sitzung. Die möglichen Werte lauten: ■ CSS-Backhaul – Für Datenverkehr, der für den Cloud-Sicherheitsdienst aus dem Edge bestimmt ist. ■ Internet-via-<*egress-iface-name*> – Für Cloud-Datenverkehr, der direkt vom Edge mithilfe einer Unternehmensrichtlinie weitergeleitet wird. ■ Internet-BH-via-<*backhaul hub name*> – Für Cloud-gebundenen Datenverkehr, der über einen Backhaul-Hub unter Verwendung einer Unternehmensrichtlinie ins Internet weitergeleitet wird. ■ <*Remote edge name*>-via-Hub – Für VPN-Datenverkehr, der über den Hub weitergeleitet wird. ■ <*Remote edge name*>-via-DE2E – Für VPN-Datenverkehr, der zwischen den Edges über einen direkten VCMP-Tunnel weitergeleitet wird. ■ <*Remote edge name*>-via-Gateway – Für VPN-Datenverkehr, der über ein Cloud-Gateway weitergeleitet wird. ■ NVS-via-<*gateway name*> – Für Non VMware SD-WAN Site-Datenverkehr, der über ein Cloud-Gateway weitergeleitet wird. ■ Internet-via-<*gateway name*> – Für Internetdatenverkehr, der über ein Cloud-Gateway weitergeleitet wird.
NAT-SRC	Die IP-Adresse der Quelle, die für die Adressübersetzung der Quelle des direkten Internetdatenverkehrs verwendet wird.

Tabelle 10-1. Felder für Firewallprotokollmeldungen (Fortsetzung)

Feld	Beschreibung
NAT-SPT	Der Quellport, der für die Portübersetzung des direkten Internetdatenverkehrs verwendet wird.
APPLICATION	Der Anwendungsname, zu dem die Sitzung von der DPI-Engine klassifiziert wurde. Dieses Feld ist nur für Meldungen für das Schließen des Protokolls verfügbar.
BYTES_SENT	Die Menge an Daten, die in Byte in der Sitzung gesendet werden. Dieses Feld ist nur für Meldungen für das Schließen des Protokolls verfügbar.
BYTES_RECEIVED	Die Menge der Daten, die in Byte in der Sitzung empfangen werden. Dieses Feld ist nur für Meldungen für das Schließen des Protokolls verfügbar.
DURATION_SECS	Die Dauer, für die die Sitzung aktiv war. Dieses Feld ist nur für Meldungen für das Schließen des Protokolls verfügbar.
REASON	Der Grund für den Abschluss oder die Ablehnung der Sitzung. Die möglichen Werte lauten: ■ State Violation ■ Reset ■ Purged ■ Aged-out ■ Fin-Received ■ RST-Received ■ Error Dieses Feld ist für die Protokollmeldungen „Schließen (Close)“ und „Ablehnen (Deny)“ verfügbar.

Konfigurieren von Cloud-VPN

Auf der Profilebene ermöglicht SD-WAN Orchestrator Ihnen die Konfiguration von Cloud-VPN (Virtual Private Network). Um VPN-Verbindungsanfragen zu initiieren und auf diese zu reagieren, müssen Sie Cloud-VPN aktivieren. Sie können Cloud-VPN über die Seite **Konfigurieren (Configure)** > **Profile (Profiles)** > **Gerät (Device)** konfigurieren.



Beim Aktivieren von Cloud-VPN für ein Profil können Sie die folgenden Cloud-VPN-Typen konfigurieren:

- Konfigurieren einer Zweigstelle für Non VMware SD-WAN Site-VPNs
- Konfigurieren von Zweigstelle-zu-SD-WAN Hubs-VPN
- Konfigurieren eines Zweigstelle-zu-Zweigstelle-VPNs

Hinweis Cloud-VPN sollte pro Segment konfiguriert werden.

Informationen zu Topologie und Anwendungsfällen finden Sie unter Cloud-VPN — Übersicht.

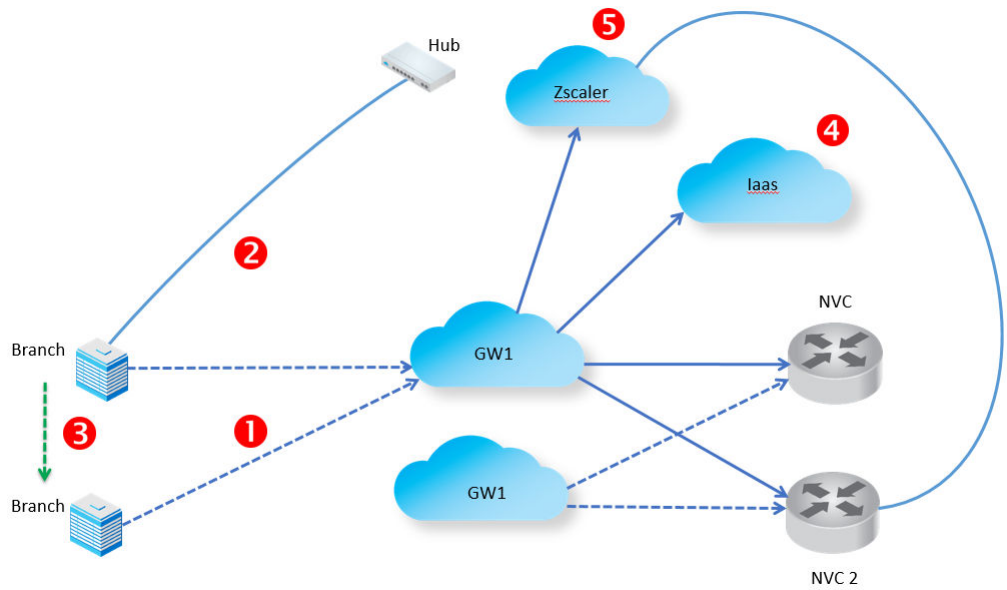
Cloud-VPN — Übersicht

Das Cloud-VPN (Virtual Private Network) ermöglicht eine VPNC-konforme IPSec-VPN-Verbindung, die VMware SD-WAN und Non VMware SD-WAN Sites miteinander verbindet. Es zeigt außerdem die Integrität der Sites an (aktiv oder inaktiv) und liefert den Echtzeitstatus der Sites.

Cloud-VPN unterstützt die folgenden Datenverkehrsströme:

- Zweigstelle-zu-Non VMware SD-WAN Site
- Zweigstelle-zu-SD-WAN Hub
- Zweigstelle-zu-Zweigstelle-VPN

Die folgende Abbildung stellt alle drei Zweige des Cloud-VPN dar. Die Zahlen in der Abbildung repräsentieren jede Zweigstelle und entsprechen den Beschreibungen in der folgenden Tabelle.



Zahl (aus obiger Abbildung)	Beschreibung
1	Non VMware SD-WAN Site

2	Zweigstelle-zu-SD-WAN Hub
3	Zweigstelle-zu-Zweigstelle-VPN
4	Zweigstelle-zu-Non VMware SD-WAN Site
5	Zweigstelle-zu-Non VMware SD-WAN Site

Zweigstelle-zu-Non VMware SD-WAN Site

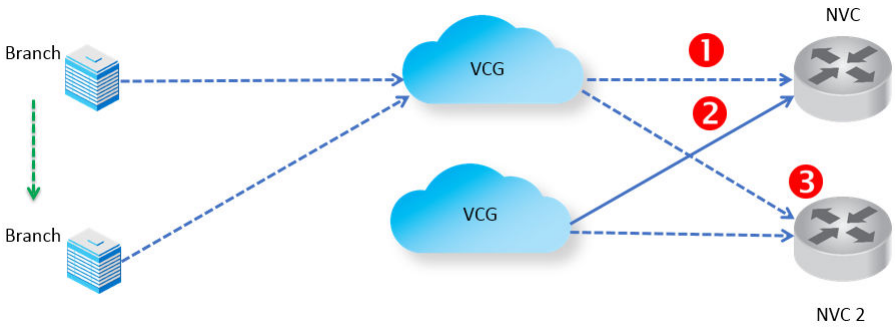
Zweigstelle-zu-Non VMware SD-WAN Site unterstützt die folgenden Konfigurationen:

- Verbindung mit Kundendatencenter mit vorhandenem Firewall-VPN-Router
- laas
- Verbindung mit CWS (Zscaler)

Verbindung mit Kundendatencenter mit vorhandenem Firewall-VPN-Router

Eine VPN-Verbindung zwischen dem VMware SD-WAN-Gateway und der Datencenter-Firewall (beliebiger VPN-Router) bietet Konnektivität zwischen den Zweigstellen (mit SD-WAN Edges installiert) und Non VMware SD-WAN Sites, was wiederum zu einer einfachen Implementierung führt. Dies bedeutet, dass keine Installation des Kundendatencenters erforderlich ist.

Die folgende Abbildung zeigt eine VPN-Konfiguration:



Zahl (aus obiger Abbildung)	Beschreibung
1	Primärer Tunnel
2	Redundanter Tunnel
3	Sekundäres VPN-Gateway

VMware SD-WAN unterstützt die VPN-Konnektivität mit den folgenden Firewalls von Drittanbietern:

- Cisco ASA
- Cisco ISR
- PaloAlto
- SonicWall
- Generischer Router (routerbasiertes VPN)
- Generische Firewall (richtlinienbasiertes VPN)

Informationen zum Konfigurieren einer Zweigstelle-zu-Non VMware SD-WAN Site finden Sie unter Konfigurieren einer Non VMware SD-WAN Site.

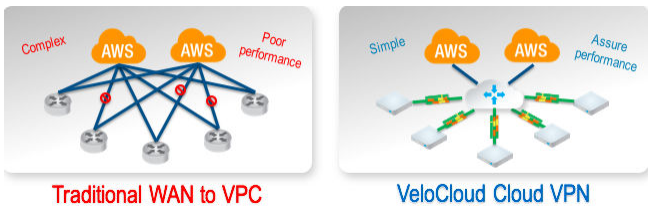
Iaas

Verwenden Sie beim Konfigurieren mit Amazon Web Services (AWS) die Option „Generische Firewall (richtlinienbasiertes VPN) (Generic Firewall (Policy Based VPN))“ im Dialogfeld „Non VMware SD-WAN Site“.

Die Konfiguration mit einer Drittpartei kann Ihnen auf folgende Weise Vorteile bringen:

- Eliminiert Mesh
- Kosten
- Leistung

Wie in der folgenden Abbildung dargestellt, ist ein VMware SD-WAN-Cloud-VPN im Vergleich zu einem herkömmlichen WAN zu VPC einfach einzurichten (globale Netzwerke von SD-WAN Gateways eliminieren die Mesh-Tunnel-Anforderung an VPCs), es verfügt über eine zentrale Richtlinie zur Kontrolle des VPC-Zugriffs von Zweigstellen, gewährleistet die Leistung und sichert die Konnektivität.



Informationen zur Konfiguration mithilfe von Amazon Web Services (AWS) finden Sie im Abschnitt Konfigurieren von Amazon Web Services.

Verbindung mit CWS (Zscaler)

Zscaler Web Security bietet Sicherheit, Sichtbarkeit und Kontrolle. Zscaler wird in der Cloud bereitgestellt und bietet Websicherheit mit Funktionen wie Bedrohungsschutz, Echtzeit-Analyse und Forensik.

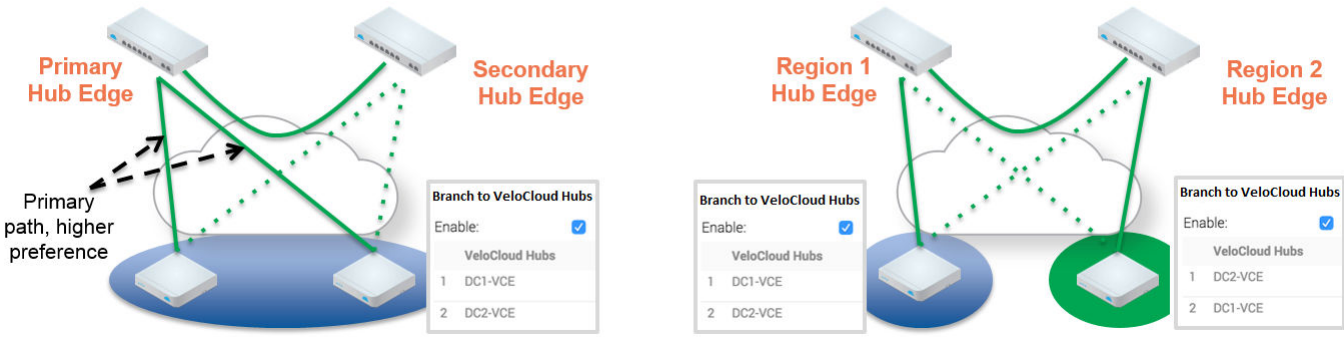
Die Konfiguration mithilfe von Zscaler bietet die folgenden Vorteile:

- **Leistung:** Direkt zu Zscaler (Zscaler über Gateway)
- **Die Proxy-Verwaltung ist komplex:** Ermöglicht Zscaler mit einfacher Klick-Richtlinie

Zweigstelle-zu-SD-WAN Hub

Der SD-WAN Hub ist ein Edge, der in Datencentern eingesetzt wird, damit Zweigstellen auf die Ressourcen von Datencentern zugreifen können. Sie müssen Ihren SD-WAN Hub auf der SD-WAN Orchestrator-Instanz einrichten. Die SD-WAN Orchestrator-Instanz benachrichtigt alle SD-WAN Edges-Instanzen über die Hubs, und die SD-WAN Edges-Instanzen erstellen sichere Overlay-Tunnel mit mehreren Pfaden zu den Hubs.

Die folgende Abbildung zeigt, wie sowohl „Aktiv-Standby“ als auch „Aktiv-Aktiv“ unterstützt werden.



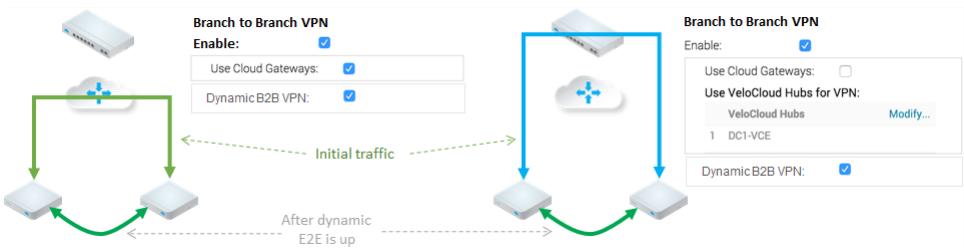
Zweigstelle-zu-Zweigstelle-VPN

Das Zweigstelle-zu-Zweigstelle-VPN unterstützt Konfigurationen für das Herstellen einer VPN-Verbindung zwischen Zweigstellen zur Verbesserung der Leistung und Skalierbarkeit.

Das Zweigstelle-zu-Zweigstelle-VPN unterstützt zwei Konfigurationen:

- Cloud-Gateways
- SD-WAN Hubs für VPN

Die folgende Abbildung zeigt die Zweigstelle-zu-Zweigstelle-Datenverkehrsströme sowohl für Cloud-Gateway als auch für einen SD-WAN Hub.



Sie können auch „Dynamisches Zweigstelle-zu-Zweigstelle-VPN (Dynamic Branch to Branch VPN)“ für die Cloud-Gateways und Hubs aktivieren.

Sie können auch auf die Funktion „Cloud-VPN mit einem Klick (1-click Cloud VPN)“ zugreifen, indem Sie in SD-WAN Orchestrator die Option **Konfigurieren (Configure) > Profile (Profiles) > Registerkarte „Gerät“ (Device Tab)** im Bereich **Cloud-VPN (Cloud VPN)** auswählen.

Hinweis Schrittweise Anleitungen zum Konfigurieren von Cloud-VPN finden Sie unter Konfigurieren von Cloud-VPN.

Konfigurieren einer Zweigstelle für Non VMware SD-WAN Site-VPNs

Konfigurieren Sie eine Zweigstelle für Non VMware SD-WAN Site-VPNs, um eine VPN-Verbindung zwischen einer Zweigstelle und einer Non VMware SD-WAN Site zu herzustellen.

Verfahren

1 Navigieren Sie in SD-WAN Orchestrator zu **Konfigurieren (Configure)** > **Profile (Profiles)**.

Die Seite **Konfigurationsprofile (Configuration Profiles)** wird angezeigt.

2 Wählen Sie ein Profil aus, in dem Sie Cloud-VPN konfigurieren möchten, und klicken Sie auf das Symbol unter der Spalte **Gerät (Device)**.

Die Seite **Geräteeinstellungen (Device Settings)** wird für das ausgewählte Profil angezeigt.

3 Navigieren Sie zum Bereich **Cloud-VPN (Cloud VPN)** und aktivieren Sie Cloud-VPN, indem Sie die Umschaltfläche auf **Ein (On)** festlegen.

4 Um eine Zweigstelle für die Non VMware SD-WAN Site zu konfigurieren, aktivieren Sie unter **Zweigstelle für Nicht-VeloCloud-Site (Branch to Non-VeloCloud Site)** das Kontrollkästchen **Aktivieren (Enable)**.

5 Wählen Sie im Dropdown-Menü eine Non VMware SD-WAN Site aus, um eine VPN-Verbindung herzustellen. Klicken Sie auf das Pluszeichen **+**, um eine weitere Non VMware SD-WAN Sites hinzuzufügen.

6 Sie können auch VPN-Verbindungen erstellen, indem Sie die Option **Neue Nicht-VeloCloud-Site (New Non-VeloCloud Site)** aus dem Dropdown-Menü auswählen. Das Dialogfeld **Neue Nicht-VeloCloud-Site (New Non-VeloCloud Site)** wird angezeigt.

a Geben Sie im Textfeld **Name** den Namen für die Non VMware SD-WAN Site ein.

b Wählen Sie im Dropdown-Menü **Typ (Type)** eine Non VMware SD-WAN Site aus.

c Geben Sie im Textfeld **Primäres VPN-Gateway (Primary VPN Gateway)** die IP-Adresse ein, die Sie als primäres VPN-Gateway für die ausgewählte Non VMware SD-WAN Site konfigurieren möchten.

d Klicken Sie auf **Weiter (Next)**. Es wird eine neue Non VMware SD-WAN Site erstellt und dem Non VMware SD-WAN Site-Dropdown-Menü hinzugefügt.

Weitere Informationen zum Konfigurieren einer Non VMware SD-WAN Site finden Sie unter Konfigurieren einer Non VMware SD-WAN Site.

7 Klicken Sie auf **Änderungen speichern (Save Changes)**.

Hinweis Das Zweigstelle-zu-Non VMware SD-WAN Site-VPN sollte erst aktiviert werden, wenn das Gateway für das Unternehmens-Datencenter vom Administrator des Unternehmens-Datencenters konfiguriert und der VPN-Tunnel des Datencenters aktiviert wurde.

Konfigurieren von Zweigstelle-zu-SD-WAN Hubs-VPN

Konfigurieren Sie Zweigstelle-zu-SD-WAN Hubs-VPN, um eine VPN-Verbindung zwischen Zweigstelle und Hubs herzustellen.

Verfahren

1 Navigieren Sie in SD-WAN Orchestrator zu **Konfigurieren (Configure)** > **Profile (Profiles)**.

Die Seite **Konfigurationsprofile (Configuration Profiles)** wird angezeigt.

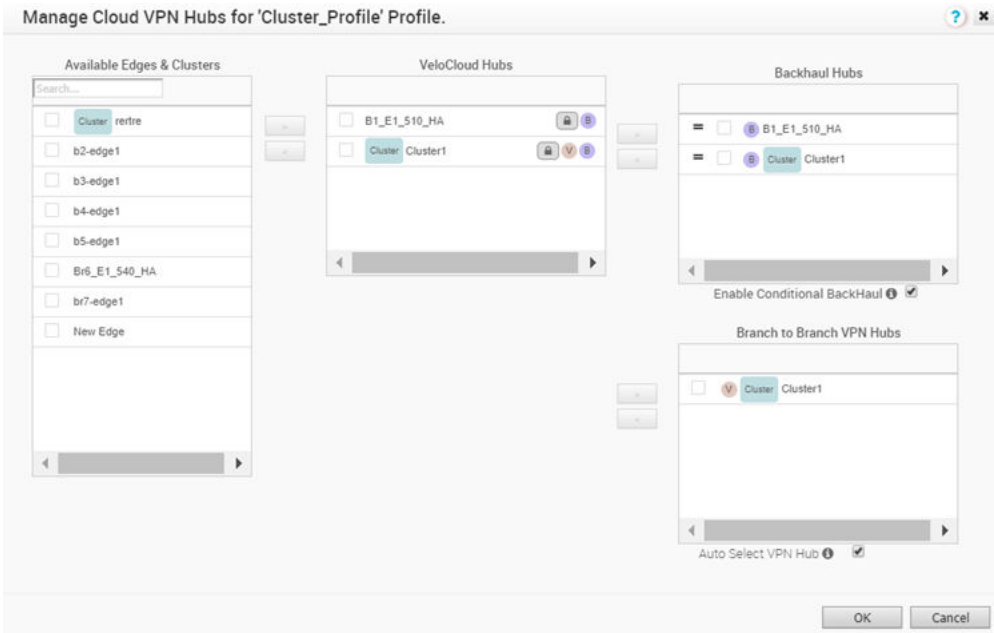
2 Wählen Sie ein Profil aus, in dem Sie Cloud-VPN konfigurieren möchten, und klicken Sie auf das Symbol unter der Spalte **Gerät (Device)**.

Die Seite **Geräteeinstellungen (Device Settings)** wird für das ausgewählte Profil angezeigt.

3 Navigieren Sie zum Bereich **Cloud-VPN (Cloud VPN)** und aktivieren Sie Cloud-VPN, indem Sie die Umschaltfläche auf **Ein (On)** festlegen.

4 Aktivieren Sie zum Konfigurieren von Zweigstelle-zu-SD-WAN Hubs unter **Zweigstelle-zu-VeloCloud-Hubs (Branch to VeloCloud Hubs)** das Kontrollkästchen **Aktivieren (Enable)**.

5 Klicken Sie auf den Link **VeloCloud Hubs auswählen (Select VeloCloud Hubs)**. Die Seite **Cloud-VPN-Hubs verwalten (Manage Cloud VPN Hubs)** wird für das ausgewählte Profil angezeigt.



6 Unter **Verfügbare Edges und Cluster (Available Edges & Clusters)** können Sie die Edges auswählen und konfigurieren, die als SD-WAN Hubs oder Backhaul-Hubs eingesetzt werden sollen. Wahlweise können Sie im Zweigstellenprofil Zweigstelle-zu-Zweigstelle-VPN-Hubs auswählen, indem Sie die Pfeilschaltfläche **>** oder **<** verwenden.

Hinweis Ein Edge-Cluster und ein einzelner Edge können gleichzeitig als Hubs in einem Zweigstellenprofil konfiguriert werden. Sobald Edges einem Cluster zugewiesen sind, können sie nicht mehr als einzelne Hubs zugewiesen werden.

Hinweis Zweigstelle-zu-Zweigstelle-VPN mit Hubs funktioniert unabhängig davon, ob es sich um Cluster oder einzelne Edges handelt. Zum Konfigurieren von Zweigstelle-zu-Zweigstelle-VPN mit Hubs, die auch-Edge-Cluster sind, können Sie einen Hub aus dem Bereich **VeloCloud-Hubs (VeloCloud Hubs)** auswählen und ihn in den Bereich **Zweigstelle-zu-Zweigstelle-VPN-Hubs (Branch to Branch VPN Hubs)** verschieben. Es wird empfohlen, das Kontrollkästchen **VPN-Hub automatisch auswählen (Auto Select VPN Hub)** zu aktivieren, sodass der Edge den besten Hub für die Herstellung der Zweigstelle-zu-Zweigstelle-Hub-Verbindung auswählt.

7 Zum Aktivieren von bedingtem Backhaul aktivieren Sie das Kontrollkästchen **Bedingtes Backhaul aktivieren (Enable Conditional BackHaul**).

Wenn der bedingte Backhaul (CBH) aktiviert ist, kann der Edge ein Failover von internetgebundenem Datenverkehr (direkter Internetdatenverkehr, Internet über SD-WAN Gateway und Datenverkehr für Cloud-Sicherheit über IPsec) zu MPLS-Verbindungen durchführen, wenn keine öffentlichen Internetverbindungen verfügbar sind. Wenn die Funktion „Bedingter Backhaul“ aktiviert ist, unterliegen standardmäßig alle Unternehmensrichtlinienregeln auf der Zweigstellenebene dem Failover des Datenverkehrs über bedingten Backhaul. Sie können den Datenverkehr vom bedingten Backhaul basierend auf bestimmten Anforderungen für ausgewählte Richtlinien ausschließen, indem Sie diese Funktionen auf der ausgewählten Unternehmensrichtlinienebene deaktivieren. Weitere Informationen finden Sie unter Bedingter Backhaul.

8 Klicken Sie auf **Änderungen speichern (Save Changes)**.

Bedingter Backhaul

Bedingter Backhaul (Conditional Backhaul, CBH) ist eine Funktion, die für die Bereitstellung von Hybrid SD-WAN-Zweigstellen entwickelt wurde, die über mindestens eine öffentliche und eine private Verbindung verfügen. Bei einem Ausfall der öffentlichen Internetverbindung auf einem VMware SD-WAN Edge werden keine Tunnel zu VMware SD-WAN Gateway, kein Cloud-Sicherheitsdienst (Cloud Security Service, CSS) und kein direkter Breakout zum Internet eingerichtet. In diesem Szenario nutzt die Funktion „Bedingter Backhaul“, wenn sie aktiviert ist, die Konnektivität über private Verbindungen zu bestimmten Backhaul-Hubs. Dadurch erhält der SD-WAN Edge die Möglichkeit, ein Failover des internetgebundenen Datenverkehrs über private Overlays an den Hub durchzuführen und die Erreichbarkeit von Internetzielen zu gewährleisten.

Immer dann, wenn eine öffentliche Internetverbindung ausfällt und der bedingte Backhaul aktiviert ist, kann der Edge ein Failover der folgenden internetgebundenen Datenverkehrstypen durchführen:

1 Direkt zum Internet

2 Internet über SD-WAN Gateway

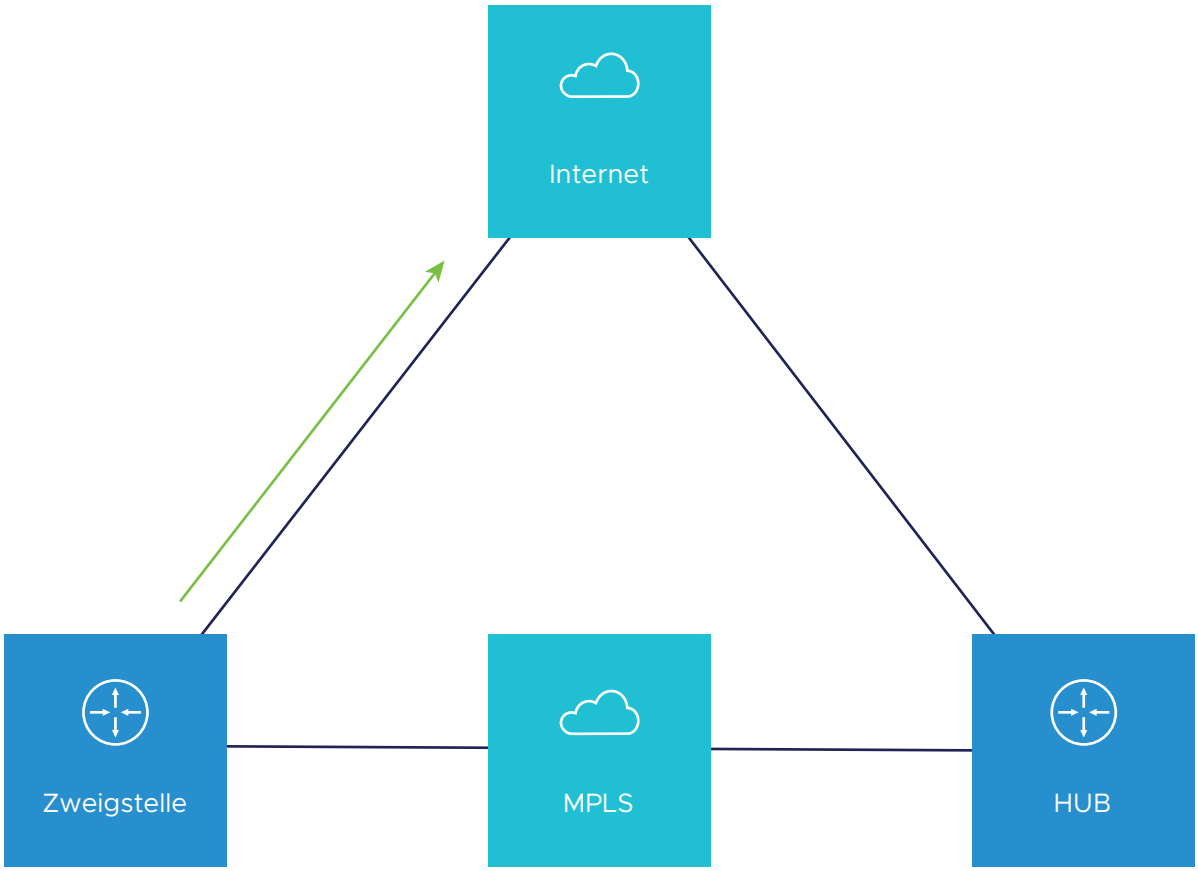
3 Datenverkehr des Cloud-Sicherheitsdiensts

Verhaltenseigenschaften des bedingten Backhauls

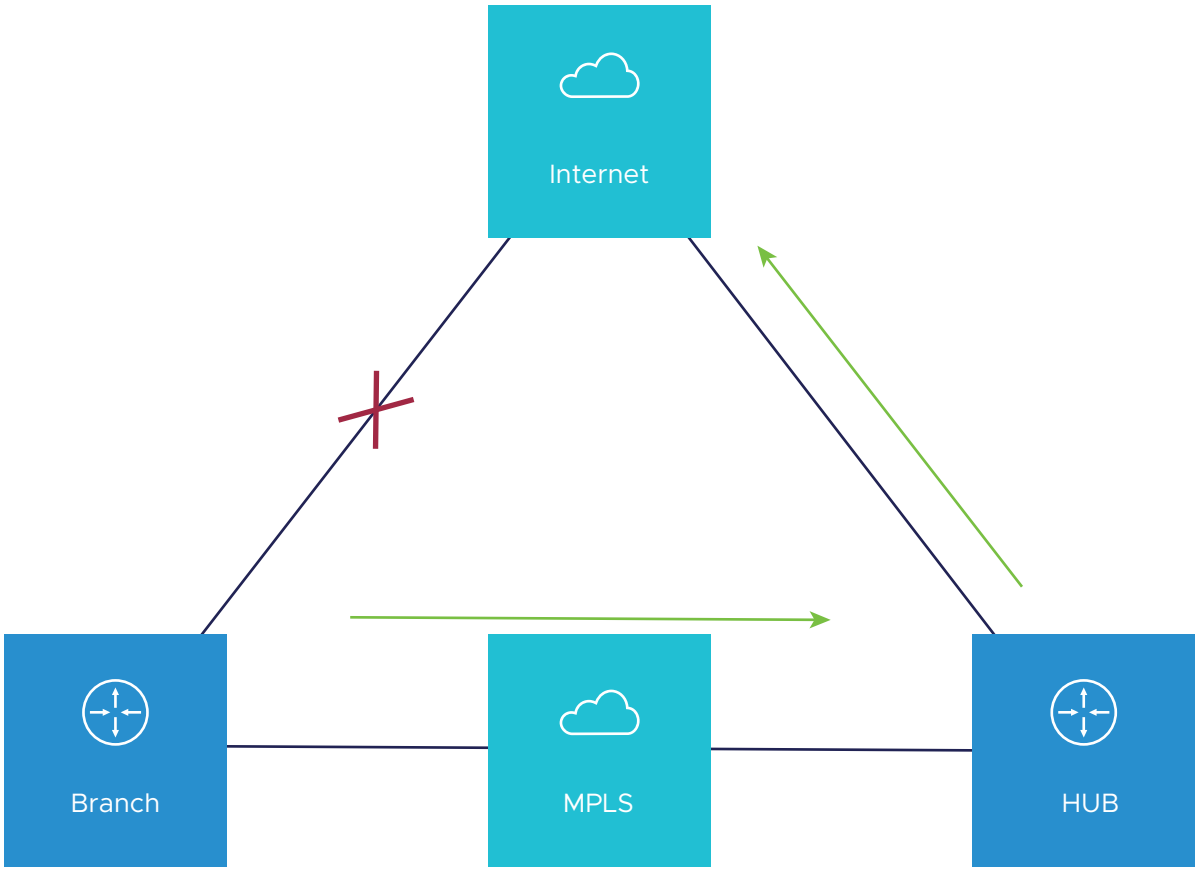
- Wenn die Funktion „Bedingter Backhaul“ aktiviert ist, unterliegen standardmäßig alle Unternehmensrichtlinienregeln auf der Zweigstellenebene dem Failover des Datenverkehrs über CBH. Sie können den Datenverkehr vom bedingten Backhaul basierend auf bestimmten Anforderungen für ausgewählte Richtlinien ausschließen, indem Sie diese Funktionen auf der ausgewählten Unternehmensrichtlinienebene deaktivieren.
- Der bedingte Backhaul wirkt sich nicht auf vorhandene Flows aus, die bereits im Hintergrund auf einen Hub zurückgeleitet werden, wenn die öffentliche Verbindung ausfällt bzw. die öffentlichen Verbindungen ausfallen. Die vorhandenen Flows leiten weiterhin Daten über denselben Hub weiter.
- Wenn ein Zweigstellenstandort über Backups öffentlicher Verbindungen verfügt, hat das Backup der öffentlichen Verbindung Vorrang vor CBH. Nur wenn alle primären und Backup-Verbindungen nicht funktionsfähig sind, wird der CBH ausgelöst und die private Verbindung verwendet.
- Wenn eine private Verbindung als Backup fungiert, wird mithilfe der CBH-Funktion ein Failover des Datenverkehr zu der privaten Verbindung durchgeführt, wenn die aktive private Verbindung ausfällt und die private Backup-Verbindung aktiv wird.
- Damit die Funktion korrekt arbeitet, müssen sowohl Zweigstellen als auch CBH-Hubs (Conditional Backhaul, bedingter Backhaul) den gleichen privaten Netzwerknamen für ihre privaten Verbindungen haben. (Andernfalls wird der Tunnel „Privat“ nicht aktiviert.)

Betriebsablauf

Unter normalen Umständen ist die öffentliche Verbindung verfügbar, und der internetgebundene Datenverkehr fließt normal entweder direkt oder über SD-WAN Gateway gemäß den konfigurierten Unternehmensrichtlinieneinstellungen.



Wenn die öffentliche Internetverbindung ausfällt oder der SD-WAN-Overlay-Pfad in den Ruhezustand (QUIET-Zustand) versetzt wird (vom Gateway werden nach 7 Taktsignalen keine Pakete empfangen), wird der internetgebundene Datenverkehr dynamisch zum Hub zurückgeleitet.

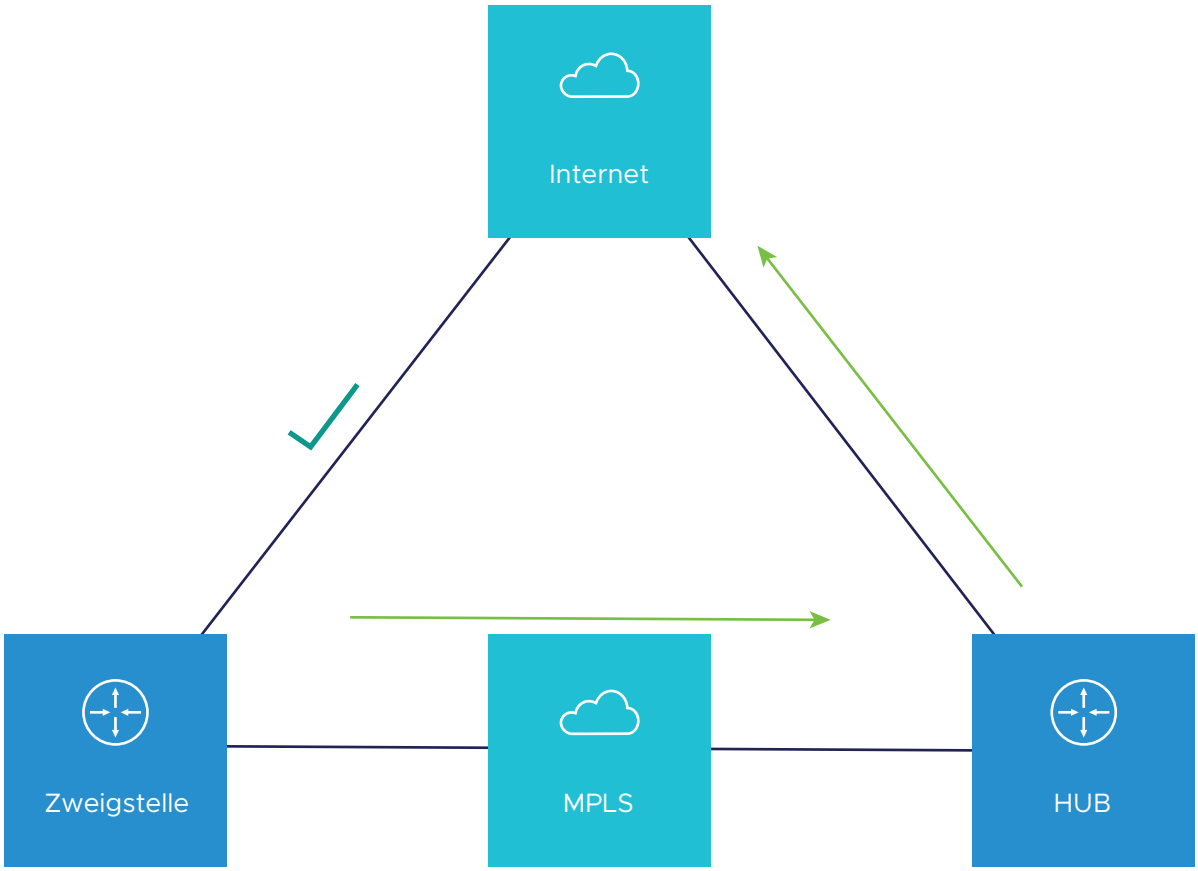


Die auf dem Hub konfigurierte Unternehmensrichtlinie bestimmt, wie dieser Datenverkehr weitergeleitet wird, sobald er den Hub erreicht. Es gibt folgende Optionen:

- Direkt vom Hub
- Hub zu Gateway und anschließend Breakout vom Gateway

Wenn die öffentliche Internetverbindung wieder aktiv ist, versucht CBH die Flows wieder zu der öffentlichen Verbindung zu verschieben. Um zu vermeiden, dass eine instabile Verbindung dazu führt, dass der Datenverkehr zwischen der öffentlichen und der privaten Verbindung ins Stocken gerät, verfügt CBH standardmäßig über einen 30-Sekunden-Holdoff-Timer. Nachdem der Holdoff-Timer erreicht ist, erfolgt ein Failback der Flows zu der öffentlichen Internetverbindung.

.



Konfigurieren von bedingtem Backhaul

Um einen bedingten Backhaul zu konfigurieren, sollten Sie auf der Profilebene Cloud-VPN aktivieren und dann eine VPN-Verbindung zwischen Zweigstelle und SD-WAN-Hubs herstellen, indem Sie die folgenden Schritte ausführen:

1 Navigieren Sie in SD-WAN Orchestrator zu **Konfigurieren (Configure)** > **Profile (Profiles)**. Die Seite **Konfigurationsprofile (Configuration Profiles)** wird angezeigt.

2 Wählen Sie ein Profil aus, in dem Sie Cloud-VPN konfigurieren möchten, und klicken Sie auf das Symbol unter der Spalte „Gerät (Device)“. Die Seite „Geräteeinstellungen (Device Settings)“ wird für das ausgewählte Profil angezeigt.

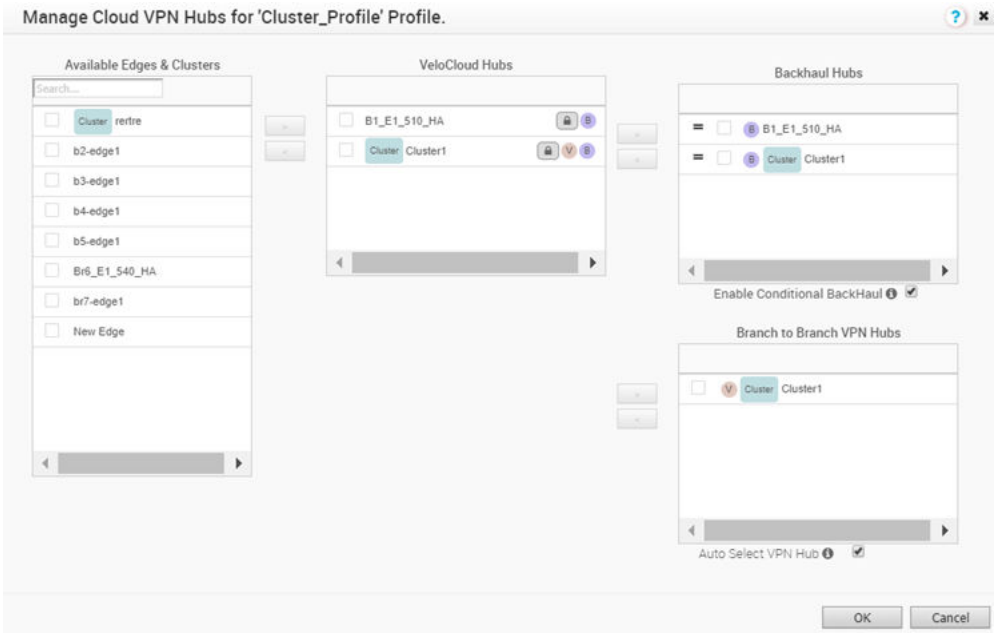
3 Wählen Sie im Dropdown-Menü **Segment konfigurieren (Configure Segment)** ein Profilsegment aus, um den bedingten Backhaul zu konfigurieren. Standardmäßig ist **Globales Segment [Normal] (Global Segment [Regular])** ausgewählt.

Hinweis Die Funktion „Bedingter Backhaul“ ist segmentfähig und muss daher in jedem Segment aktiviert werden, in dem sie funktionieren soll.

4 Navigieren Sie zum Bereich **Cloud-VPN (Cloud VPN)** und aktivieren Sie Cloud-VPN, indem Sie die Umschaltfläche auf **Ein (On)** festlegen.

5 Aktivieren Sie zum Konfigurieren von Zweigstelle-zu-SD-WAN Hubs unter **Zweigstelle-zu-VeloCloud-Hubs (Branch to VeloCloud Hubs)** das Kontrollkästchen **Aktivieren (Enable)**.

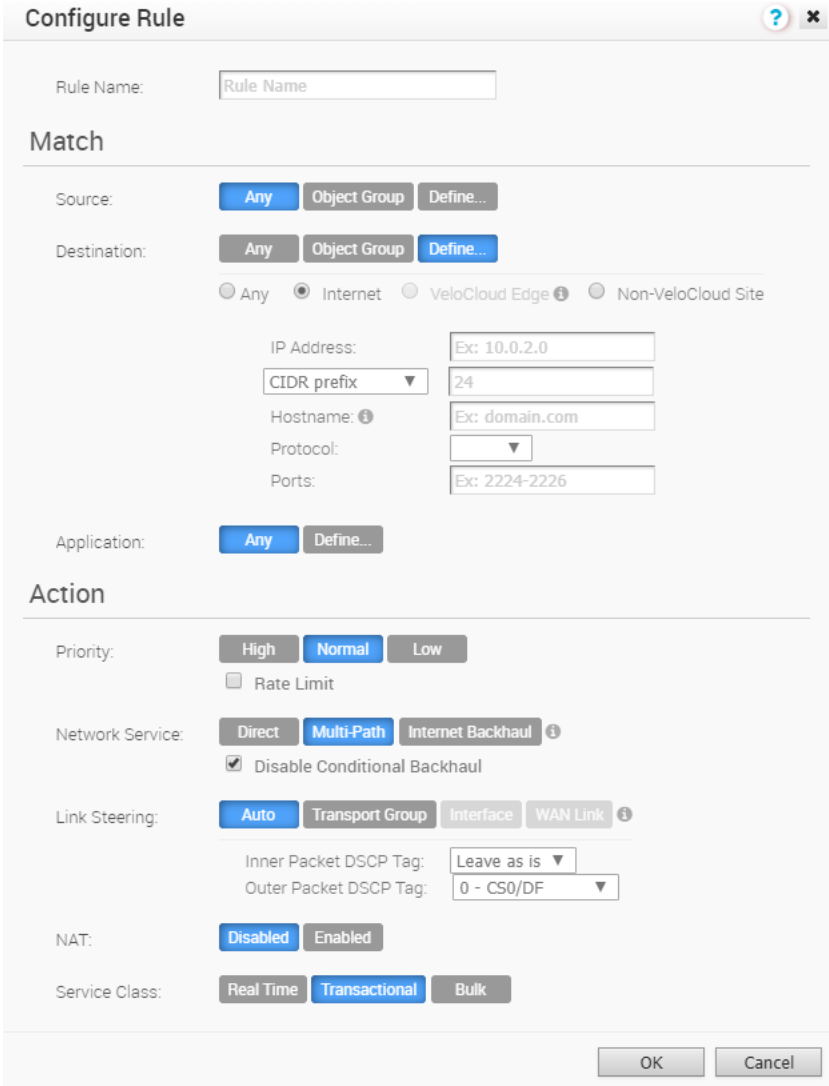
6 Klicken Sie auf den Link **VeloCloud Hubs auswählen (Select VeloCloud Hubs)**. Die Seite **Cloud-VPN-Hubs verwalten (Manage Cloud VPN Hubs)** wird für das ausgewählte Profil angezeigt.



Wählen Sie im Bereich **VeloCloud-Hubs (VeloCloud Hubs)** die Hubs aus, die als Backhaul-Hubs fungieren sollen, und verschieben Sie sie mit der Pfeilschaltfläche **>** in den Bereich **Backhaul-Hubs (Backhaul Hubs)**.

7 Zum Aktivieren von bedingtem Backhaul aktivieren Sie das Kontrollkästchen **Bedingtes Backhaul aktivieren (Enable Conditional BackHaul**).

Wenn der bedingte Backhaul aktiviert ist, kann der Edge ein Failover von internetgebundenem Datenverkehr (direkter Internetdatenverkehr, Internet über SD-WAN Gateway und Datenverkehr für Cloud-Sicherheit über IPsec) zu MPLS-Verbindungen durchführen, wenn keine öffentlichen Internetverbindungen verfügbar sind. Bedingter Backhaul wird bei Aktivierung standardmäßig für alle Unternehmensrichtlinien angewendet. Wenn Sie Datenverkehr vom bedingten Backhaul basierend auf bestimmten Anforderungen ausschließen möchten, können Sie den bedingten Backhaul für ausgewählte Richtlinien deaktivieren, um ausgewählten Datenverkehr von diesem Verhalten auszuschließen. Aktivieren Sie dazu das Kontrollkästchen **Bedingten Backhaul deaktivieren (Disable Conditional Backhaul)** im Bereich **Aktion (Action)** im Bildschirm **Regel konfigurieren (Configure Rule)** für die ausgewählte Unternehmensrichtlinie.



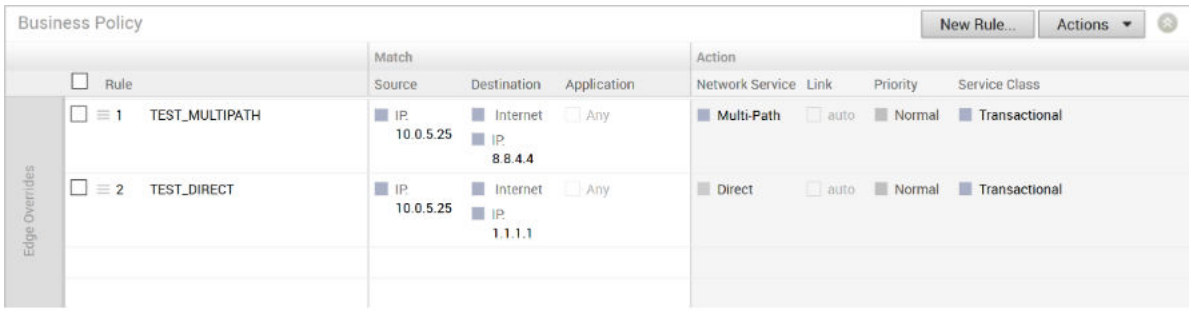
Hinweis

- Der bedingte Backhaul und die SD-WAN-Erreichbarkeit können in demselben Edge zusammenarbeiten. Sowohl der bedingte Backhaul als auch die SD-WAN-Erreichbarkeit unterstützen das Failover von Cloud-gebundenem Gateway-Datenverkehr zu MPLS, wenn das öffentliche Internet auf dem Edge ausgefallen ist. Wenn der bedingte Backhaul aktiviert ist und es keinen Pfad zum Gateway und einen Pfad zum Hub über MPLS gibt, gilt der bedingte Backhaul sowohl für den direkten als auch für den Gateway-gebundenen Datenverkehr. Weitere Informationen zur Erreichbarkeit von SD-WAN finden Sie unter Erreichbarkeit des SD-WAN-Diensts über MPLS.
- Wenn mehrere Kandidaten-Hubs vorhanden sind, verwendet der bedingte Backhaul den ersten Hub in der Liste, es sei denn, die Verbindung zwischen Hub und Gateway ist unterbrochen.

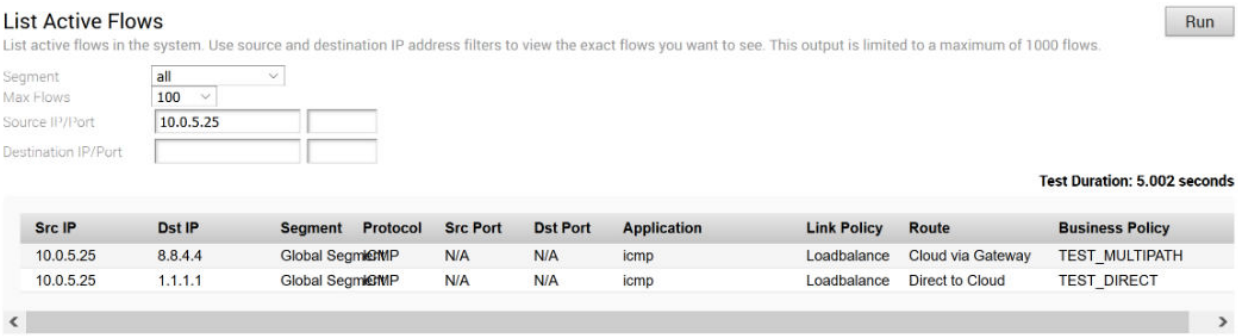
8 Klicken Sie auf **Änderungen speichern (Save Changes)**.

Fehlerbehebung bei bedingtem Backhaul

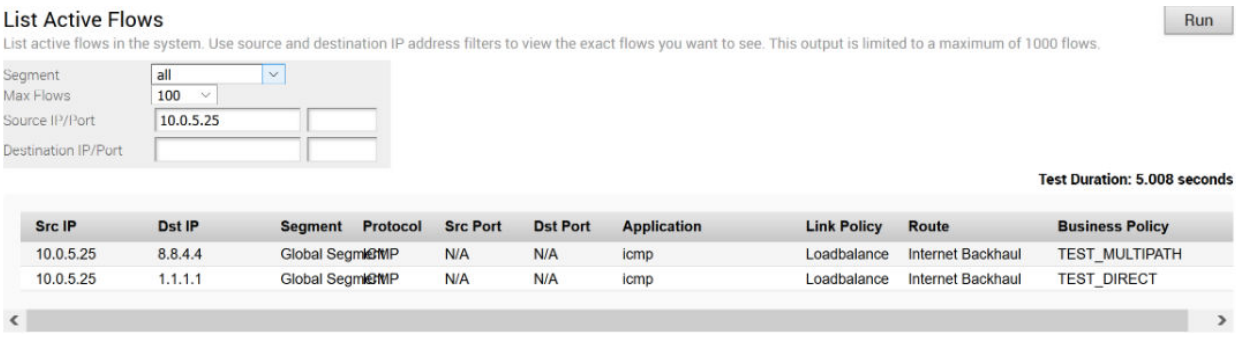
Angenommen, ein Benutzer hat die folgenden zwei Unternehmensrichtlinienregeln auf Zweigstellenebene erstellt.



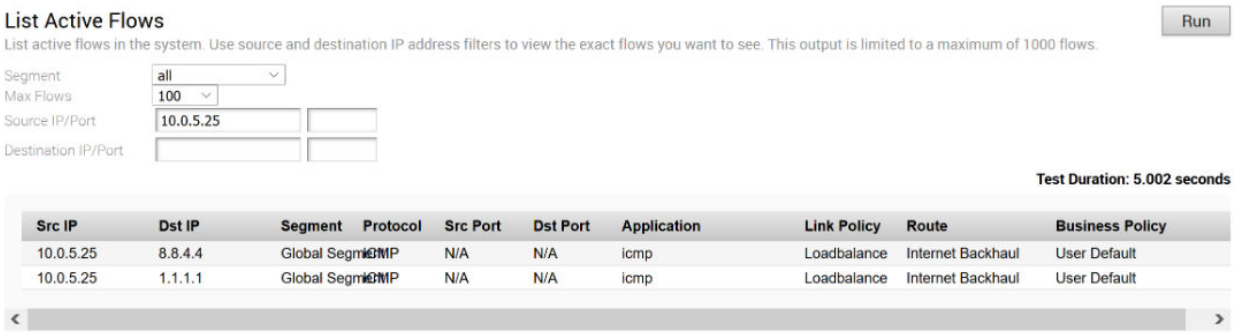
Sie können überprüfen, ob die konstanten Pings an jede dieser Ziel-IP-Adressen für die Zweigstelle aktiv sind, indem Sie im Abschnitt „Remote-Diagnose (Remote Diagnostics)“ den Befehl **Aktive Flows auflisten (List Active Flows)** ausführen.



Falls in der öffentlichen Verbindung der Zweigstelle ein extremer Paketverlust auftritt und die Verbindung unterbrochen ist, wechseln dieselben Flows in der Zweigstelle zu Internet-Backhaul.



Beachten Sie, dass die Unternehmensrichtlinie auf dem Hub bestimmt, wie der Hub den Datenverkehr weiterleitet. Da der Hub keine bestimmte Regel für diese Flows aufweist, werden sie als Standarddatenverkehr kategorisiert. In diesem Szenario kann eine Unternehmensrichtlinienregel auf der Hub-Ebene erstellt werden, die den gewünschten IPs oder Subnetzbereichen entspricht, um festzulegen, wie Flows von einer bestimmten Zweigstelle gehandhabt werden, falls CBH einsatzbereit wird.



Konfigurieren eines Zweigstelle-zu-Zweigstelle-VPNs

Konfigurieren Sie ein Zweigstelle-zu-Zweigstelle-VPN, um eine VPN-Verbindung zwischen den Zweigstellen herzustellen.

Verfahren

1 Klicken Sie im Unternehmensportal auf **Konfigurieren (Configure)** > **Profile (Profiles)**.

Die Seite **Konfigurationsprofile (Configuration Profiles)** wird angezeigt.

2 Wählen Sie ein Profil aus, in dem Sie Cloud-VPN konfigurieren möchten, und klicken Sie auf das Symbol unter der Spalte **Gerät (Device)**.

Die Seite **Geräteeinstellungen (Device Settings)** wird für das ausgewählte Profil angezeigt.

3 Navigieren Sie zum Bereich **Cloud-VPN (Cloud VPN)** und aktivieren Sie Cloud-VPN, indem Sie die Umschaltfläche auf **Ein (On)** festlegen.

4 Um ein Zweigstelle-zu-Zweigstelle-VPN zu konfigurieren, aktivieren Sie unter **Zweigstelle-zu-Zweigstelle-VPN (Branch to Branch VPN)** das Kontrollkästchen **Aktivieren (Enable)**.

Das Zweigstelle-zu-Zweigstelle-VPN unterstützt zwei Konfigurationen für die Einrichtung einer VPN-Verbindung zwischen Zweigstellen:

Konfiguration	Beschreibung
Verwenden von SD-WAN Gateway	Bei dieser Option wird das nächstgelegene Gateway zum Einrichten von VPN-Verbindungen zwischen Edges verwendet. Das SD-WAN Gateway kann Datenverkehr von anderen Benutzern aufweisen.
Verwenden von SD-WAN Hub	Bei dieser Option werden ein oder mehrere Edges als Hubs ausgewählt, die VPN-Verbindungen zwischen den Zweigstellen herstellen können. Der Hub wird Ihr Asset sein und nur Ihre Unternehmensdaten enthalten, wodurch die Sicherheit insgesamt verbessert wird.

5 Zum Aktivieren der Profilisolierung aktivieren Sie das Kontrollkästchen **Profil isolieren (Isolate Profile)**.

Wenn die Profilisolierung aktiviert ist, lernen die Edges innerhalb des Profils keine Routen von anderen Edges außerhalb des Profils über das SD-WAN-Overlay.

Sie können dynamisches Zweigstelle-zu-Zweigstelle-VPN auf allen Edges oder Edges innerhalb eines Profils aktivieren. Bei Aktivierung des Kontrollkästchens **Aktiviert (Enabled)** wird standardmäßig für alle Edges das dynamische Zweigstelle-zu-Zweigstelle-VPN konfiguriert. Stellen Sie zum Konfigurieren von dynamischem Zweigstelle-zu-Zweigstelle-VPN nach Profil sicher, dass das Kontrollkästchen **Profil isolieren (Isolate Profile)** deaktiviert ist.

Hinweis Wenn die Profilisolierung aktiviert ist, kann dynamisches Zweigstelle-zu-Zweigstelle-VPN nur für Edges innerhalb des Profils aktiviert werden.

Wenn Sie Dynamisches Zweigstelle-zu-Zweigstelle-VPN (Dynamic Branch to Branch VPN) aktivieren, durchläuft das erste Paket das Cloud-Gateway (oder den Hub). Wenn der initiierende Edge feststellt, dass Datenverkehr durch einen sicheren Overlay-Mehrfachpfad-Tunnel weitergeleitet werden kann, und wenn „Dynamisches Zweigstelle-zu-Zweigstelle-VPN (Dynamic Branch to Branch VPN)“ aktiviert ist, wird ein direkter Tunnel zwischen den Zweigstellen erstellt.

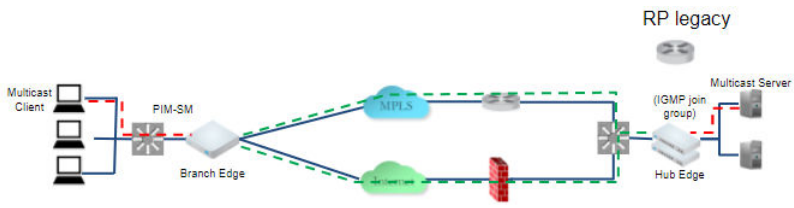
Sobald der Tunnel eingerichtet ist, beginnt der Datenverkehr über den sicheren Overlay-Mehrfachpfad-Tunnel zwischen den Zweigstellen zu fließen. Nach 180 Sekunden ohne Datenverkehr (vorwärts oder rückwärts von beiden Seiten der Zweigstellen) wird der Tunnel durch das Initiieren des Edge wieder abgebaut.

6 Klicken Sie auf **Änderungen speichern (Save Changes)**.

Konfigurieren von Multicast-Einstellungen

Multicast bietet eine effiziente Möglichkeit, Daten an eine interessierte Gruppe von Empfängern zu senden, indem nur eine Kopie der Daten von der Quelle aus gesendet wird. Hierfür replizieren die zwischengeschalteten Multicast-Router im Netzwerk Pakete, um mehrere Empfänger basierend auf einem Gruppenabonnement zu erreichen.

Multicast-Clients verwenden das Internet Group Management Protocol (IGMP) zur Weitergabe von Mitgliedschaftsinformationen von Hosts an Multicast-fähige Router und PIM zur Weitergabe von Gruppenmitgliedsinformationen an Multicast-Server über Multicast-Router.



Die Multicast-Unterstützung umfasst Folgendes:

- Multicast-Unterstützung auf dem Overlay und dem Underlay

- Protokollunabhängiger Multicast – Sparse-Modus (PIM-SM) auf SD-WAN Edge
- IGMP-Version 2 (Internet Group Management Protocol) auf SD-WAN Edge
- Konfiguration des statischen Rendezvous-Punkts (RP), wobei RP auf einem Router eines Drittanbieters aktiviert ist.

Globale Konfiguration von Multicast

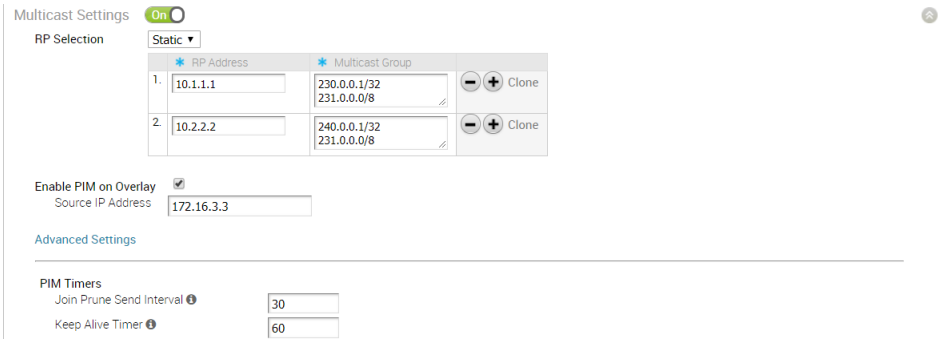
Es gibt zwei Schritte zum Aktivieren und Konfigurieren von Multicast (global und auf Schnittstellenebene), die beide auf Edge-Ebene außer Kraft gesetzt werden können. Die nachfolgend aufgeführten Schritte enthalten Anweisungen dazu, wie Sie Multicast global aktivieren können.

So konfigurieren Sie Multicast global:

1 Navigieren Sie von **Konfigurieren > Profil > Geräte (Configure > Profile > Devices)** zum Bereich **Multicast-Einstellungen (Multicast Settings)**.

2 Wenn sich die Schaltfläche **Multicast-Einstellungen (Multicast Settings)** in der Position **Aus (Off)** befindet, klicken Sie auf die Schaltfläche **Aus (Off)**, um die Multicast-Einstellungen zu aktivieren.

   Die Auswahl des RP ist standardmäßig auf **Statisch (Static)** festgelegt.



3 Geben Sie in die entsprechenden Textfelder für die RP-Auswahl die RP-Adresse und die Multicast-Gruppe ein. (In der folgenden Tabelle finden Sie eine Beschreibung der **RP-Adresse (RP Address)** und der **Multicast-Gruppe (Multicast Group)**).

4 Aktivieren Sie ggf. das Kontrollkästchen **PIM auf Overlay aktivieren (Enable PIM on Overlay)** und geben Sie die IP-Quelladresse ein.

5 Legen Sie bei Bedarf **Erweiterte Einstellungen (Advanced Settings)** fest. Eine Beschreibung der einzelnen Einstellungen finden Sie in der folgenden Tabelle. Geben Sie in die entsprechenden Textfelder PIM-Timer für **Sendeintervall zum Hinzufügen/Entfernen (Join Prune Send Interval)** (Standard 60 Sekunden) und **Keep Alive-Timer (Keep Alive Timer)** (Standard 60 Sekunden) ein.

Multicast-Einstellungen

In der folgenden Tabelle sind die Multicast-Einstellungen beschrieben.

Multicast-Einstellung	Beschreibung
RP-Auswahl (RP Selection)	Konfigurieren Sie RP für Multicast-Gruppen. **Statischer RP (Static RP)** ist der standardmäßige unterstützte Mechanismus in der Version 3.2.
PIM auf Overlay aktivieren (Enable PIM on Overlay)	Aktivieren Sie PIM-Peering auf SD-WAN Overlay. Ist dies beispielsweise sowohl auf dem Branch-SD-WAN Edge als auch auf dem Hub-SD-WAN Edge aktiviert, bilden diese einen PIM-Peer. Standardmäßig wird die Quell-IP-Adresse für die Overlays von einer der Multicast-fähigen Underlay-Schnittstellen abgeleitet, und es wird empfohlen, die Standardeinstellung beizubehalten. Benutzer können die Quell-IP-Adresse optional ändern, indem sie die **Quell-IP-Adresse (Source IP Address)** angeben. Dabei handelt es sich um eine virtuelle Adresse, die automatisch über den Overlay angekündigt wird.
PIM-Timer (PIM Timers)	
Sendeintervall zum Hinzufügen/Entfernen (Join Prune Send Interval)	Der Timer des Intervalls zum Hinzufügen/Entfernen. Der Standardwert beträgt 60 Sekunden.
Keep Alive-Timer (Keep Alive Timer)	PIM-Keep-Alive-Timer. Der Standardwert beträgt 60 Sekunden.

Konfigurieren der Multicast-Einstellungen auf der Schnittstellenebene

So aktivieren und konfigurieren Sie Multicast auf der Schnittstellenebene:

1 Wählen Sie auf der Registerkarte **Profilgerät konfigurieren (Configure Profiles Device)** des Bildschirms ein Ziel-Edge-Modell aus und navigieren Sie zum Bereich „Schnittstelleneinstellungen (Interfaces Settings)“ und wählen Sie die Schnittstelle aus, für die Sie Multicast aktivieren möchten.

2 Klicken Sie auf die Schaltfläche **Bearbeiten (Edit)**, um das Dialogfeld **Schnittstelleneinstellungen (Interface Settings)** für den von Ihnen konfigurierten Edge zu öffnen.

3 Geben Sie im Dialogfeld **Schnittstelle (Interface)** das Edge-Modell ein:

   a Aktivieren Sie das Kontrollkästchen **Schnittstelle aktiviert (Interface Enabled)**, um die Einstellungen für das Dialogfeld anzuzeigen.

   b Wählen Sie im Dropdown-Menü **Funktionalität (Capability)** die Option **Weitergeleitet (Routed)** aus, um die Einstellungen für Multicast verwenden zu können.

   c Wählen Sie im Dropdown-Menü **Adresstyp (Addressing Type)** entweder „DHCP“, „PPPoE“ oder „Statisch (Static)“ aus.

   d Aktivieren Sie ggf. das Kontrollkästchen **WAN-Overlay (WAN Overlay)**.

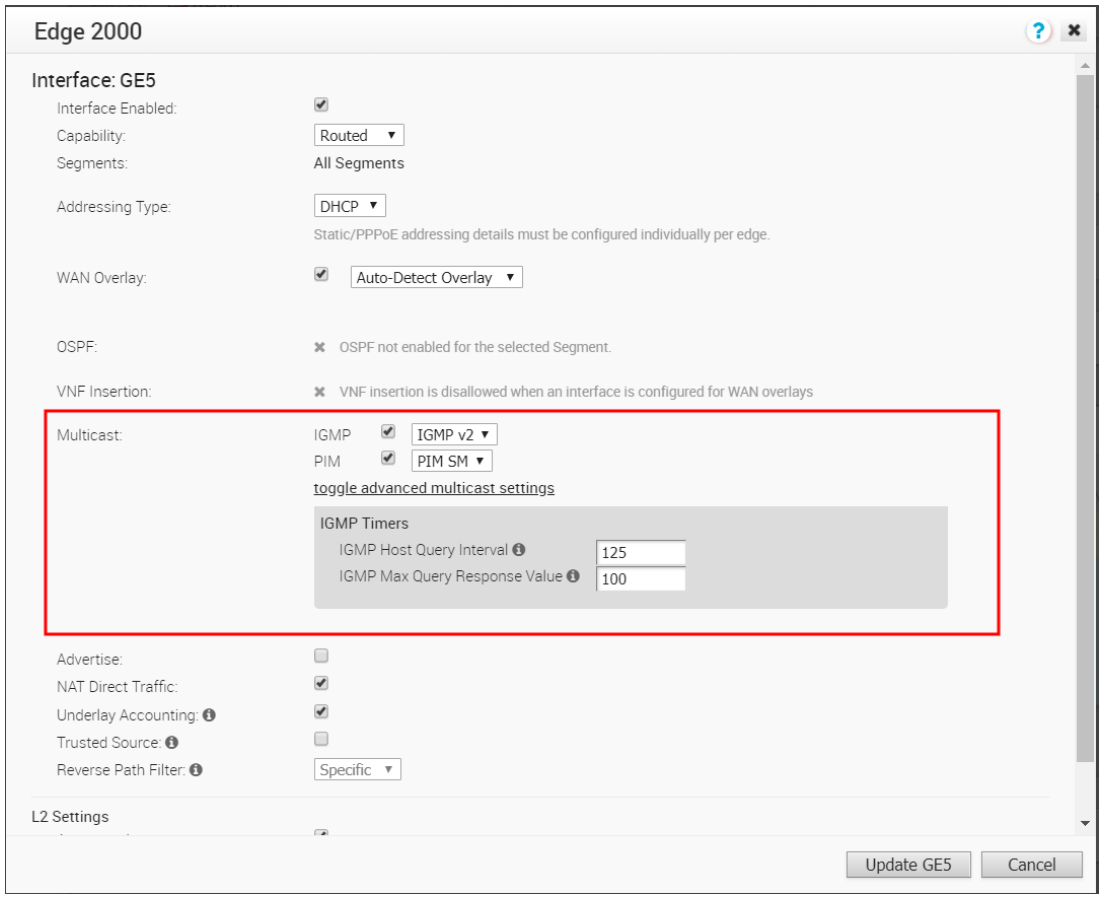
   e Aktivieren Sie ggf. das Kontrollkästchen **OSPF**.

   f Gehen Sie im Abschnitt **Multicast** wie folgt vor:

      1 Aktivieren Sie ggf. das Kontrollkästchen **IGMP** und wählen Sie die einzige verfügbare Option „IGMP v2“ aus.

      2 Aktivieren Sie ggf. das Kontrollkästchen **PIM** und wählen Sie die einzige verfügbare Option „PIM SM“ aus.

3 Klicken Sie auf den Link **Erweiterte Multicast-Einstellungen umschalten (toggle advanced multicast settings)**, um die IGMP-Timer einzustellen, wie in der Abbildung unten gezeigt.



- IGMP-Host-Abfrageintervall (IGMP Host Query Interval): Der Standardwert beträgt 125 Sekunden und der Bereich 1-1800.
- Maximaler IGMP-Abfrageantwortwert (IGMP Max Query Response Value): Der Standardwert beträgt 100 Dezisekunden und der Bereich 10-250.

g Falls zutreffend, aktivieren Sie die folgenden Kontrollkästchen: „Ankündigen (Advertise)“, „Direkter NAT-Datenverkehr (NAT Direct Traffic)“, „Underlay-Berechnung (Underlay Accounting)“ und „Vertrauenswürdige Quelle (Trusted Source)“.

h Nehmen Sie im Dropdown-Menü **Umgekehrter Pfadfilter (Reverse Path Filter)** eine Auswahl vor (**Deaktiviert (Disabled)**, **Spezifisch (Specific)**, **Unspezifisch (Loose)**). **HINWEIS:** Der Benutzer kann den umgekehrten Pfadfilter nur dann festlegen, wenn die vertrauenswürdige Zone aktiviert ist. Wenn die vertrauenswürdige Zone nicht aktiviert ist, wird standardmäßig der Wert **Spezifisch (Specific)** angezeigt, wie in der obigen Abbildung dargestellt.

i Aktivieren Sie im Bereich **L2-Einstellungen (L2 Settings)**, sofern zutreffend, das Kontrollkästchen **Autom. aushandeln (Autonegotiate)**. Geben Sie ggf. die MTU in das Textfeld ein.

j Wenn „Autom. aushandeln (Autonegotiate)“ nicht ausgewählt ist, geben Sie die **Geschwindigkeit (Speed)**, **Duplex** und **MTU** in die entsprechenden Kontrollkästchen ein.

k Klicken Sie für das Edge-Modell auf **Aktualisieren (Update)**.

Die folgende Tabelle beschreibt die IGMP-Timer.

IGMP-Timer	Beschreibung
IGMP-Host-Abfrageintervall	IGMP-Host-Abfrageintervall, Standardwert ist 60 Sekunden.
Maximaler IGMP-Abfrageantwortwert	Maximaler IGMP-Abfrageantwortwert, Standardwert ist 10 Sekunden.

Hinweis Navigieren Sie zur Registerkarte **Überwachen (Monitor) > Routing > Multicast**, um Informationen zum Multicast-Routing anzuzeigen. Weitere Informationen finden Sie unter Überwachen des Routings.

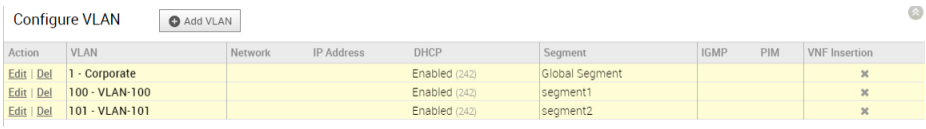
Konfigurieren von VLAN für Profile

Als Unternehmensadministrator können Sie ein VLAN auf Profilebene konfigurieren.

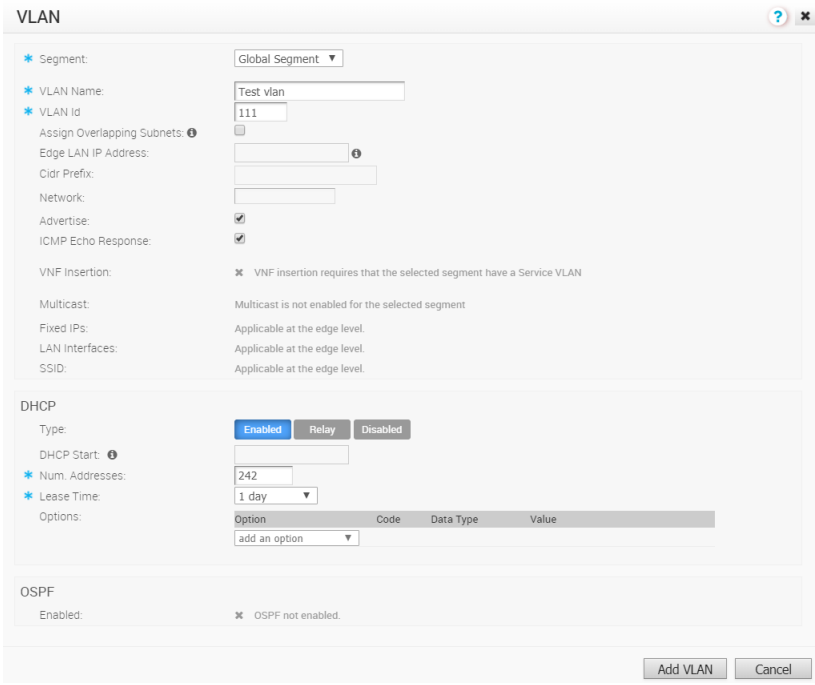
Führen Sie die folgenden Schritte aus, um ein neues VLAN auf Profilebene hinzuzufügen:

1 Navigieren Sie in SD-WAN Orchestrator zu **Konfigurieren (Configure)** > **Profile (Profiles)**. Die Seite **Konfigurationsprofile (Configuration Profiles)** wird angezeigt.

2 Wählen Sie ein Profil aus, um ein VLAN zu konfigurieren, und klicken Sie auf das Symbol in der Spalte **Gerät (Device)**. Die Seite „Geräteeinstellung (Device Setting)“ für das ausgewählte Profil wird angezeigt.



3 Navigieren Sie zum Bereich **VLAN konfigurieren (Configure VLAN)** und klicken Sie auf **VLAN hinzufügen (Add VLAN)**.



4 Konfigurieren Sie im Dialogfeld **VLAN** die folgenden Details:

a Wählen Sie im Dropdown-Menü **Segment** ein Profilsegment aus, um das VLAN zu konfigurieren.

b Geben Sie im Textfeld **VLAN-Name (VLAN Name)** einen eindeutigen Namen für das VLAN ein.

c Geben Sie im Textfeld **VLAN-ID (VLAN ID)** eine eindeutige ID für das VLAN ein.

d Aktivieren Sie das Kontrollkästchen **Überlappende Subnetze zuweisen (Assign Overlapping Subnets)**, wenn Sie allen Edges im Profil dasselbe Subnetz für das VLAN zuweisen möchten. Durch Aktivierung dieses Kontrollkästchens können Sie ein für alle Edges im Profil zu verwendendes Subnetz definieren, indem Sie die Felder **Edge-LAN-IP-Adresse (Edge LAN IP Address)** und **Cidr-Präfix (Cidr Prefix)** verwenden. Die Adresse unter **Netzwerk (Network)** wird auf Basis der Subnetzmaske und des CIDR-Werts automatisch eingerichtet.

Hinweis Wenn Sie allen Edges verschiedene Subnetze zuweisen möchten (z. B. für VPN-Netzwerke), sehen Sie von der Aktivierung des Kontrollkästchens **Überlappende Subnetze zuweisen (Assign Overlapping Subnets)** ab. Sie können die Subnetze aber auf jedem Edge einzeln konfigurieren.

e Aktivieren Sie das Kontrollkästchen **Ankündigen (Advertise)**, um das VLAN anderen Branches im Netzwerk anzukündigen.

f Aktivieren Sie das Kontrollkästchen **ICMP-Echo-Antwort (ICMP Echo Response)**, damit das VLAN auf ICMP-Echo-Meldungen antworten kann.

g Aktivieren Sie das Kontrollkästchen **VNF-Einfügung (VNF Insertion)**, um Edge-VNF-Einfügung (Virtual Network Function) zu aktivieren.

Hinweis VNF-Einfügung erfordert, dass das ausgewählte Segment ein Dienst-VLAN aufweist. Weitere Informationen zu VNF finden Sie unter Sicherheits-VNFs.

h Wenn die Funktion „Multicast“ für das ausgewählte Segment aktiviert ist, können Sie **Multicast**-Einstellungen konfigurieren, indem Sie die Kontrollkästchen **IGMP** und **PIM** aktivieren.

i Wählen Sie im Bereich **DHCP** einen der folgenden DHCP-Typen aus:

- **Aktiviert (Enabled)** – Aktiviert DHCP mit den Edges als DHCP-Server. Wenn Sie diese Option auswählen, müssen Sie die folgenden Details angeben:
  - **DHCP starten (DHCP Start)** – Geben Sie eine gültige IP-Adresse ein, die in einem Subnetz als DHCP-Start-IP verfügbar ist.
  - **Anzahl der Adressen (Num Addresses)** – Geben Sie die Anzahl der IP-Adressen ein, die in einem Subnetz auf dem DHCP-Server zur Verfügung stehen.
  - **Lease-Dauer (Lease Time)** – Wählen Sie im Dropdown-Menü den Zeitraum aus, in dem das VLAN eine IP-Adresse verwenden kann, die dynamisch vom DHCP-Server zugewiesen wurde.

  Sie können auch eine oder mehrere DHCP-Optionen hinzufügen, wenn Sie vordefinierte Optionen angeben oder benutzerdefinierte Optionen hinzufügen.
- **Relay** – Aktiviert DHCP mit dem in einem Remote-Speicherort installierten DHCP-Relay-Agenten. Wenn Sie diese Option auswählen, können Sie die IP-Adresse eines oder mehrerer Relay-Agenten angeben.
- **Deaktiviert (Disabled)** – Deaktiviert DHCP.

j Konfigurieren Sie **OSPF**-Einstellungen, wenn die OSPF-Funktion für das ausgewählte Segment aktiviert ist.

5 Klicken Sie auf **VLAN hinzufügen (Add VLAN)**. Das VLAN ist für das Profil konfiguriert. Sie können die VLAN-Einstellungen ändern, indem Sie auf den Link **Bearbeiten (Edit)** unter der Spalte **Aktionen (Actions)** klicken.

Informationen zum Konfigurieren von VLANs auf Edge-Ebene finden Sie unter Konfigurieren von VLAN für Edges.

Konfigurieren der Verwaltungs-IP-Adresse

Die **Verwaltungs-IP-Adresse (Management IP)** wird als Quelladresse für lokale Dienste (z. B. DNS) und als Ziel für Diagnosetests (z. B. das Anpingen von einem anderen Edge) verwendet.

Konfigurieren von Geräteeinstellungen

Mit den Geräteeinstellungen können Sie die Schnittstelleneinstellungen für ein oder mehrere Edge-Modelle in einem Profil konfigurieren.

Je nach Edge-Modell kann jede Schnittstelle eine Switch-Port-Schnittstelle (LAN) oder eine geroutete Schnittstelle (WAN) sein. Je nach Zweigstellen-Modell ist ein Verbindungsport ein dedizierter LAN- oder WAN-Port, oder Ports können entweder als LAN- oder WAN-Port konfiguriert werden. Zweigstellen-Ports können Ethernet- oder SFP-Ports sein. Einige Edge-Modelle unterstützen möglicherweise auch drahtlose LAN-Schnittstellen.

Es wird davon ausgegangen, dass ein einziger öffentlicher WAN-Link an eine einzige Schnittstelle angeschlossen ist, die nur den WAN-Datenverkehr bedient. Wenn für eine geroutete Schnittstelle, die WAN-fähig ist, kein WAN-Link konfiguriert ist, wird davon ausgegangen, dass ein einzelner öffentlicher WAN-Link automatisch erkannt werden soll. Wenn ein Link erkannt wird, wird er der SD-WAN Orchestrator-Instanz gemeldet. Dieser automatisch erkannte WAN-Link kann dann über die SD-WAN Orchestrator-Instanz modifiziert und die neue Konfiguration auf die Zweigstelle zurückgeschoben werden.

Hinweis

- Wenn die geroutete Schnittstelle mit dem WAN-Overlay aktiviert und mit einem WAN-Link verbunden ist, steht die Schnittstelle für alle Segmente zur Verfügung.
- Wenn eine Schnittstelle als PPPoE konfiguriert ist, unterstützt sie nur einen einzigen automatisch erkannten WAN-Link. Zusätzliche Links können nicht der Schnittstelle zugewiesen werden.

Wenn der Link nicht automatisch erkannt werden soll oder nicht erkannt werden kann, muss er explizit konfiguriert werden. Es gibt mehrere unterstützte Konfigurationen, bei denen die automatische Erkennung nicht möglich ist. Dazu zählen:

- Private WAN-Links
- Mehrere WAN-Links auf einer einzigen Schnittstelle. Beispiel: Ein Datencenter-Hub mit 2 MPLS-Verbindungen
- Ein einzelner über mehrere Schnittstellen erreichbarer WAN-Link. Beispiel: Für eine Aktiv-Aktiv-HA-Topologie

Automatisch erkannte Links sind immer öffentliche Links. Benutzerdefinierte Links können öffentlich oder privat sein und über unterschiedliche Konfigurationsoptionen verfügen, die auf dem ausgewählten Typ basieren.

Hinweis Selbst bei automatisch erkannten Links kann die Außerkraftsetzung der automatisch erkannten Parameter, wie z. B. Dienstanbieter, durch die Edge-Konfiguration überschrieben werden.

Öffentliche WAN-Links

Öffentliche WAN Links sind herkömmliche Links, die den Zugriff auf das öffentliche Internet wie z. B. Kabel, DSL usw. bieten. Für öffentliche WAN-Links ist keine Peer-Konfiguration erforderlich. Sie stellen automatisch eine Verbindung zu dem SD-WAN Gateway her, das die Weitergabe der für die Peer-Konnektivität benötigten Informationen verarbeitet.

Private WAN-Links (MPLS)

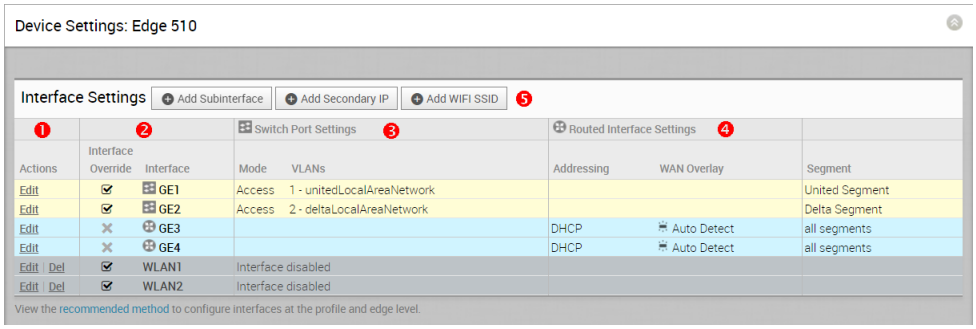
Private WAN-Links gehören zu einem privaten Netzwerk und können nur mit anderen WAN-Links in demselben privaten Netzwerk verbunden werden. Da es mehrere MPLS-Netzwerke geben kann, muss der Benutzer beispielsweise innerhalb eines einzelnen Unternehmens ermitteln, welche Links zu welchem Netzwerk gehören. Das SD-WAN Gateway verwendet diese Informationen, um die Verbindungsinformationen für die WAN-Links zu verteilen.

Sie können die MPLS-Links als einen einzelnen Link behandeln. Um jedoch zwischen verschiedenen MPLS-Dienstklassen zu unterscheiden, können mehrere WAN-Links definiert werden, die verschiedenen MPLS-Dienstklassen zugeordnet werden, indem jedem WAN-Link ein anderes DSCP-Tag zugewiesen wird.

Darüber hinaus können Sie festlegen, dass eine statische SLA für einen privaten WAN-Link definiert wird. Dadurch entfällt die Notwendigkeit für Peers, Pfadstatistiken auszutauschen, und der Bandbreitenverbrauch auf einem Link wird reduziert. Da das Prüfintervall beeinflusst, wie schnell das Gerät ausfällt, ist es nicht klar, ob eine statische SLA-Definition das Prüfintervall automatisch reduzieren soll.

Geräteeinstellungen

Die folgenden Bildschirmaufnahmen veranschaulichen die Benutzeroberfläche der obersten Ebene für den SD-WAN Edge 500, SD-WAN Edge 1000 und führen den SD-WAN Edge 610 für Version 3.4 ein. In der folgenden Tabelle werden die Hauptfunktionen der Benutzeroberfläche beschrieben (die Ziffern in der Tabelle entsprechen den Zahlen in nachfolgenden Bildschirmaufnahmen).



1. Aktionen, die Sie auf der Netzwerkschnittstelle durchführen können, wie z. B. „Bearbeiten (Edit)“ oder **Löschen (Delete)**.
2. Der Name der Schnittstelle. Dieser Name entspricht der Bezeichnung des Edge-Ports am Edge-Gerät oder ist für drahtlose LANs vorgegeben.

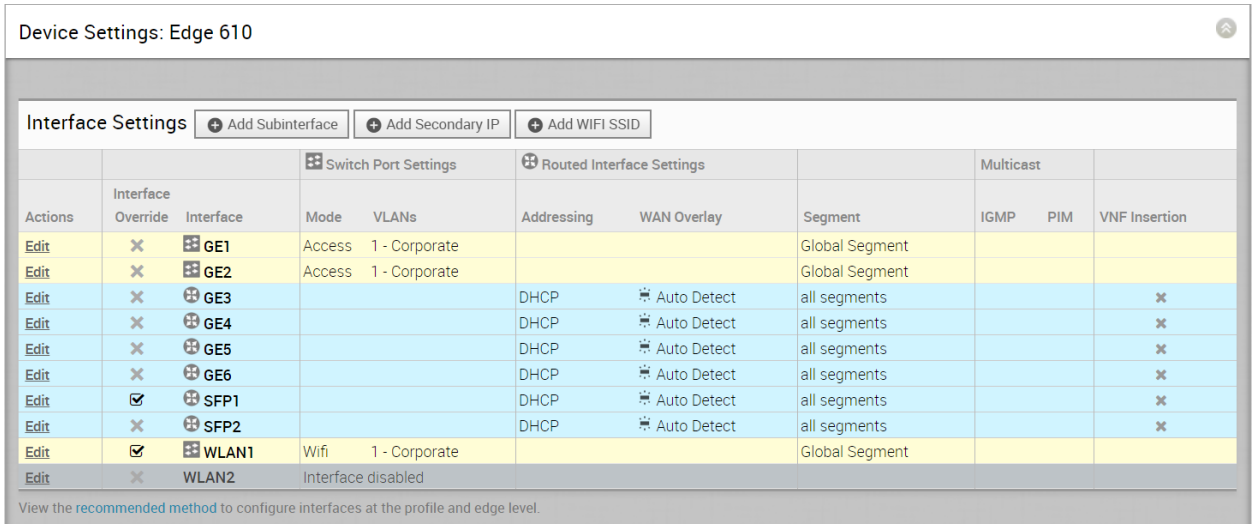
3. Die Liste der Switch-Ports mit einer Zusammenfassung einiger ihrer Einstellungen (z. B. Zugriffs- oder Trunk-Modus und die VLANs für die Schnittstelle). Switch-Ports werden mit einem hellgelben Hintergrund hervorgehoben.

4. Die Auswahl der gerouteten Schnittstellen mit einer Übersicht über ihre Einstellungen (z. B. der Adresstyp und ob die Schnittstelle automatisch erkannt wurde oder ein automatisch erkanntes oder benutzerdefiniertes WAN-Overlay aufweist). Gerouteten Schnittstellen werden mit hellblauem Hintergrund hervorgehoben.

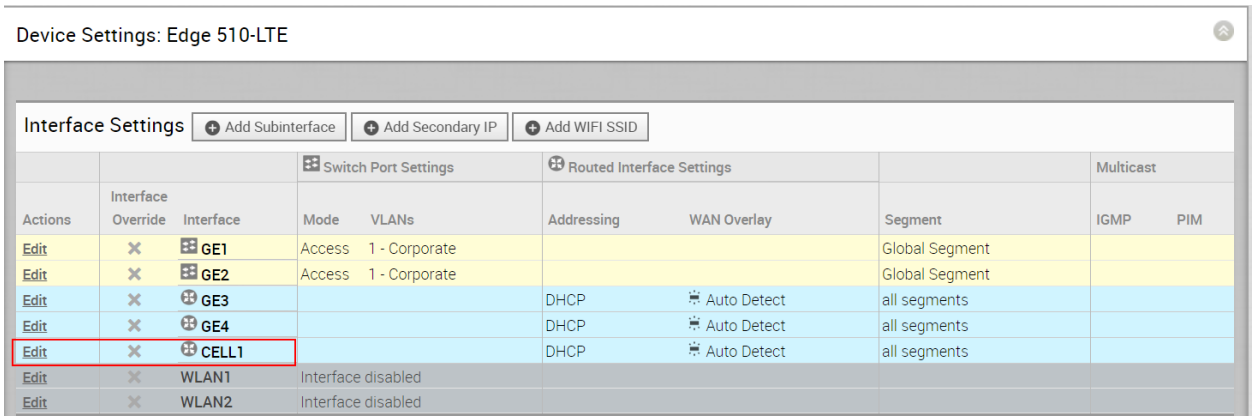
5. Die Liste der drahtlosen Schnittstellen (falls auf dem Edge-Gerät verfügbar). Sie können zusätzliche drahtlose Netzwerke hinzufügen, indem Sie auf die Schaltfläche **WLAN-SSID hinzufügen (Add Wi-Fi SSID)** klicken. Drahtlose Schnittstellen werden mit einem hellgrauen Hintergrund hervorgehoben.

5.
   - Sie können zusätzliche drahtlose Netzwerke hinzufügen, indem Sie auf die Schaltfläche **WLAN-SSID hinzufügen (Add Wi-Fi SSID)** klicken. Drahtlose Schnittstellen werden mit einem hellgrauen Hintergrund hervorgehoben.
   - Sie können Teilschnittstellen hinzufügen, indem Sie auf die Schaltfläche **Teilschnittstellen hinzufügen (Add Sub Interfaces)** klicken. Teilschnittstellen werden mit „SIF“ neben der Schnittstelle angezeigt.
   - Sie können sekundäre IPs hinzufügen, indem Sie auf die Schaltfläche **Sekundäre IP hinzufügen (Add Secondary IP)** klicken. Sekundäre IPs werden mit „SIP“ neben der Schnittstelle angezeigt.

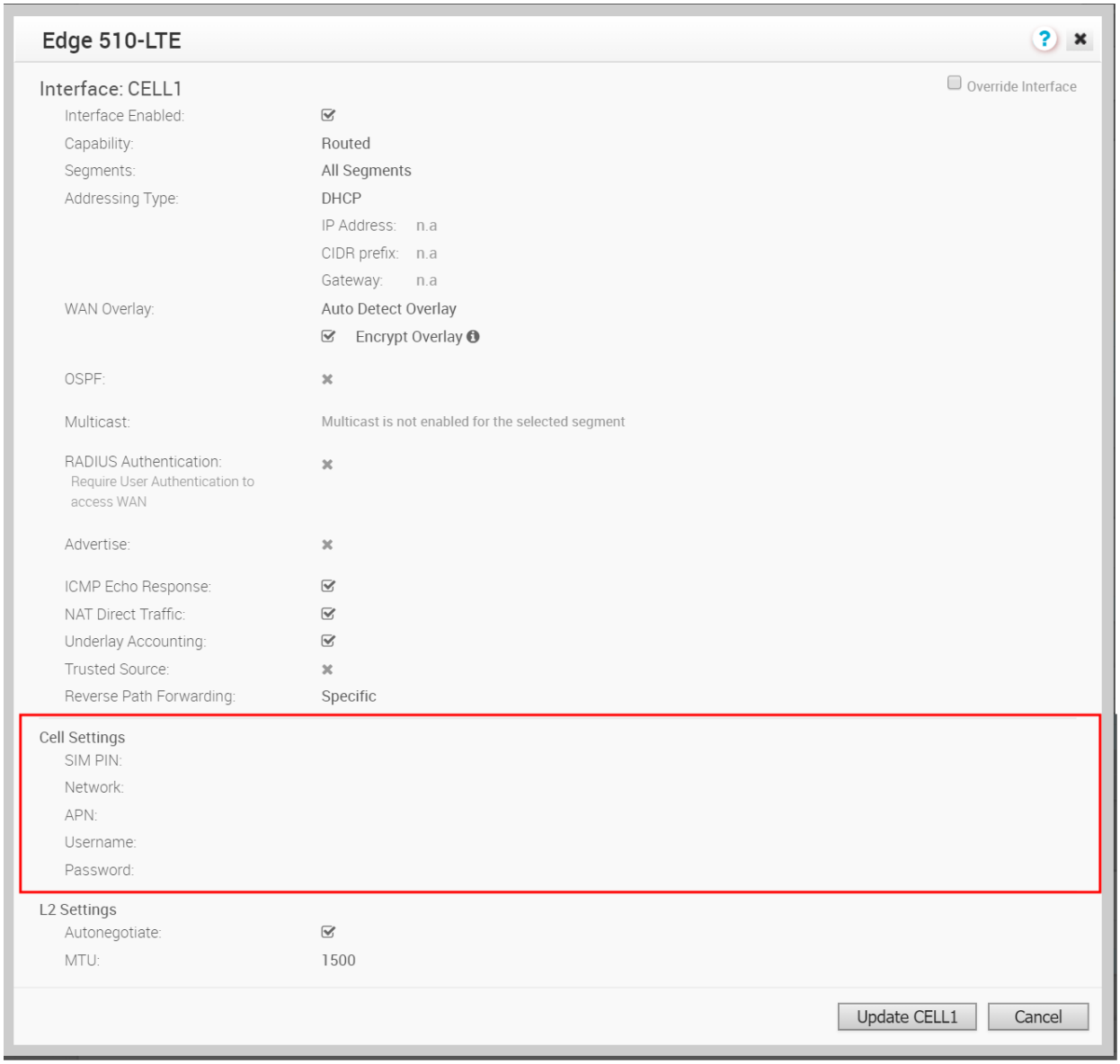
Mit der Version 3.4 wird Edge 610 eingeführt.



Für die Version 3.4 wird eine neue geroutete Schnittstelle (CELL1) hinzugefügt. Wenn Benutzer Edge 510-LTE als Modell wählen, wird diese im Bereich **Schnittstelleneinstellungen (Interface Settings)** angezeigt (siehe Abbildung unten).

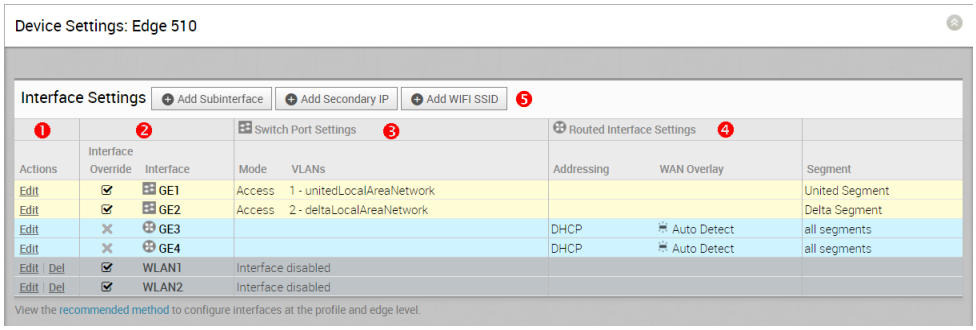


Wenn Sie auf den Link **Bearbeiten (Edit)** klicken, können Benutzer, wie in der Abbildung oben gezeigt, den Abschnitt **Zelleneinstellungen (Cell Settings)** bearbeiten. (Siehe Abbildung unten.)



Hinweis **510 Diagnosetest für LTE-Modem-Informationen (510 LTE Modem Information Diagnostic Test):** Für die Version 3.4, wenn das Edge 510 LTE-Gerät konfiguriert ist, ist der Diagnosetest „LTE-Modeminformationen (LTE Modem Information)“ verfügbar. Der Diagnosetest für LTE-Modem-Informationen ruft Diagnoseinformationen ab, wie z. B. Signalstärke, Verbindungsinformationen usw. Informationen zum Ausführen eines Diagnosetests finden Sie im Abschnitt Remote-Diagnose.

Teilschnittstellen und sekundäre IPs

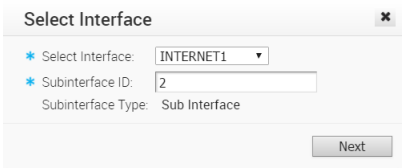


Hinzufügen einer Teilschnittstelle

Wenn Sie eine Teilschnittstelle zu einer gerouteten Schnittstelle hinzufügen, erhält die Teilschnittstelle eine Teilmenge der Konfigurationsoptionen, die der übergeordneten Schnittstelle zur Verfügung gestellt werden.

1 Klicken Sie auf die Schaltfläche **Teilschnittstelle hinzufügen (Add Sub Interface)**.

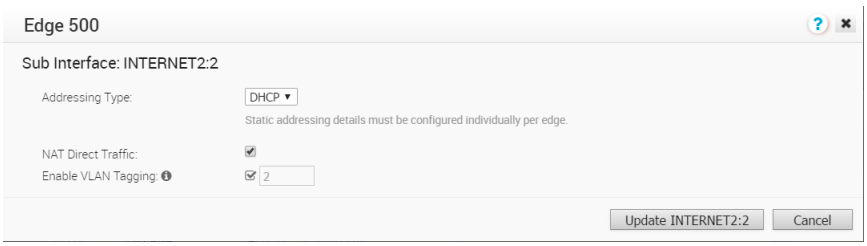
2 Wählen Sie eine Schnittstelle aus dem Dropdown-Menü und die **Teilschnittstellen-ID (Sub Interface ID)** im Textfeld aus, wie im Dialogfeld **Schnittstelle auswählen (Select Interface)** unten angezeigt.



3 Klicken Sie auf **Weiter (Next)**.

4 Wählen Sie im Dialogfeld **Teilschnittstelle (Sub Interface)** den Adresstyp aus (**DHCP** oder **Statisch (Static)**).

   a Wenn Sie den Adresstyp **DHCP** wählen, wird das Kontrollkästchen **VLAN-Tags aktivieren (Enable VLAN Tagging)** standardmäßig aktiviert, und die ID der Teilschnittstelle, die Sie im vorherigen Dialogfeld ausgewählt haben, wird im Textfeld angezeigt.



   b Wenn Sie den Adresstyp **Statisch (Static)** wählen, haben Sie die Möglichkeit, VLAN zu aktivieren, indem Sie das Kontrollkästchen **VLAN-Tags aktivieren (Enable VLAN Tagging)** aktivieren. Im Textfeld wird die ID der Teilschnittstelle angezeigt, die Sie im vorherigen Dialogfeld ausgewählt haben.

5 Aktivieren Sie bei Bedarf das Kontrollkästchen **Direkter NAT-Datenverkehr (NAT Direct Traffic)**.

6 Klicken Sie auf die Schaltfläche **Aktualisieren (Update)**.

Die Spalte **Schnittstelle (Interface)** wird aktualisiert und zeigt die neu erstellte Teilschnittstelle an.

Hinzufügen einer sekundären IP-Adresse

1 Klicken Sie auf die Schaltfläche **Sekundäre IP hinzufügen (Add Secondary IP)**.

2 Wählen Sie eine Schnittstelle aus dem Dropdown-Menü und die **Teilschnittstellen-ID (Sub Interface ID)** im Textfeld aus, wie im Dialogfeld **Schnittstelle auswählen (Select Interface)** unten angezeigt. Beachten Sie, dass der Teilschnittstellentyp „Sekundäre IP (Secondary IP)“ lautet.

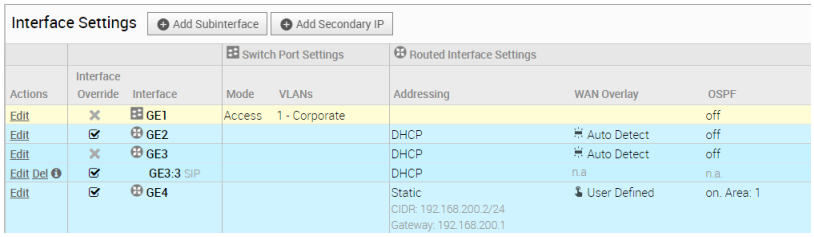
3 Klicken Sie auf **Weiter (Next)**.

4 Wählen Sie im Dialogfeld **Sekundäre IP (Secondary IP)** den Adresstyp (**DHCP** oder **Statisch (Static)**) aus.

5 Wählen Sie im Dialogfeld **Sekundäre IP (Secondary IP)** den Adresstyp (**DHCP** oder **Statisch (Static)**) aus.

6 Klicken Sie auf die Schaltfläche **Aktualisieren (Update)**.

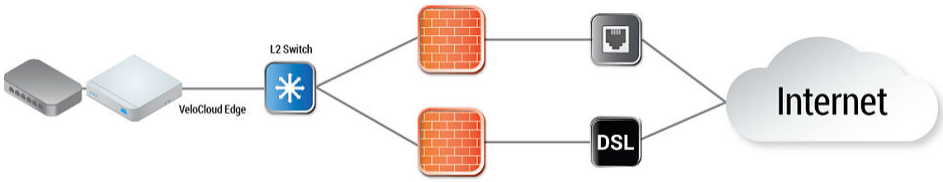
Die Spalte **Schnittstelle (Interface)** wird aktualisiert und zeigt die neu erstellte sekundäre IP an (siehe Abbildung **Schnittstelleneinstellungen (Interface Settings)** unten).



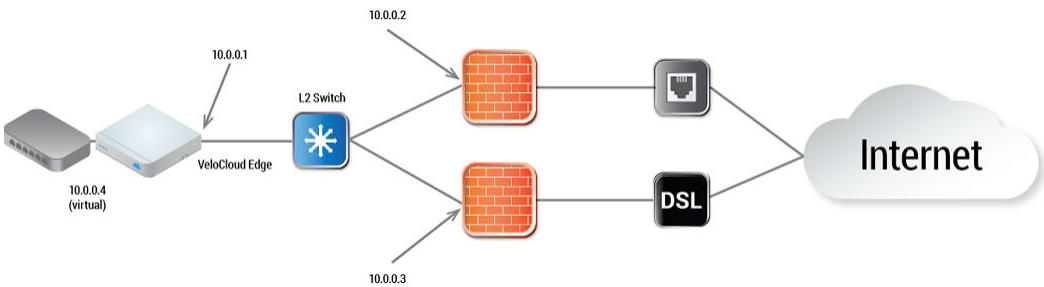
Anwendungsfälle für benutzerdefiniertes WAN-Overlay

Die Szenarien, in denen diese Konfiguration nützlich ist, werden zuerst skizziert, gefolgt von einer Spezifikation der Konfiguration selbst.

1 **Anwendungsfall 1: Zwei WAN-Links, die an einen L2-Switch angeschlossen sind**: Betrachten Sie die herkömmliche Datencenter-Topologie, bei der der SD-WAN Edge an einen L2-Switch in der DMZ angeschlossen ist, der mit mehreren Firewalls verbunden ist, die jeweils an einen anderen Upstream-WAN-Link angeschlossen sind.



In dieser Topologie wurde die VMware SD-WAN-Schnittstelle wahrscheinlich mit dem FW1 als nächster Hop konfiguriert. Um den DSL-Link nutzen zu können, muss er jedoch mit einem alternativen nächsten Hop versehen werden, an den Pakete weitergeleitet werden sollen, da FW1 die DSL nicht erreichen kann. Beim Definieren des DSL-Links muss der Benutzer eine benutzerdefinierte IP-Adresse für den nächsten Hop als IP-Adresse von FW2 konfigurieren, um sicherzustellen, dass die Pakete das DSL-Modem erreichen können. Darüber hinaus muss der Benutzer eine benutzerdefinierte IP-Adresse für dieses WAN konfigurieren, um dem Edge die Identifizierung von Rückgabeschnittstellen zu ermöglichen. Die endgültige Konfiguration ähnelt der folgenden Abbildung:

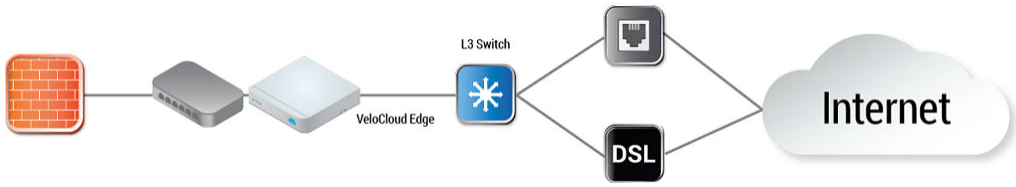


Im folgenden Abschnitt wird beschrieben, wie die endgültige Konfiguration definiert ist.

- Die Schnittstelle ist mit der IP-Adresse 10.0.0.1 und dem nächsten Hop 10.0.0.2 definiert. Da mehr als ein WAN-Link an die Schnittstelle angeschlossen ist, werden die Links auf „benutzerdefiniert (user defined)“ festgelegt.

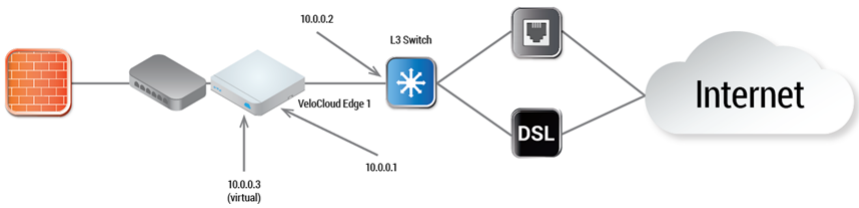
- Der Kabel-Link ist definiert und erbt die IP-Adresse von 10.0.0.1 und den nächsten Hop von 10.0.0.2. Es sind keine Änderungen erforderlich. Wenn ein Paket über den Kabel-Link gesendet werden muss, wird es von 10.0.0.1 bezogen und an das Gerät weitergeleitet, das auf ARP für 10.0.0.2 (FW1) antwortet. Rückgabepakete sind für 10.0.0.1 bestimmt und werden als auf dem Kabel-Link ankommend erkannt.
- Der DSL-Link ist definiert, und da es sich um den zweiten WAN-Link handelt, kennzeichnet die SD-WAN Orchestrator-Instanz die IP-Adresse und den nächsten Hop als obligatorische Konfigurationselemente. Der Benutzer gibt eine benutzerdefinierte virtuelle IP (z. B. 10.0.0.4) für die Quell-IP und 10.0.0.3 für den nächsten Hop an. Wenn ein Paket über den DSL-Link gesendet werden muss, wird es von 10.0.0.4 bezogen und an das Gerät weitergeleitet, das auf ARP für 10.0.0.3 (FW2) antwortet. Rückgabepakete sind für 10.0.0.4 bestimmt und werden als auf dem DSL-Link ankommend erkannt.

2 **Anwendungsfall 2: Zwei WAN-Links, die an einen L3-Switch/Router angeschlossen sind**: Alternativ kann das Upstream-Gerät ein L3-Switch oder ein Router sein. In diesem Fall ist das nächste Hop-Gerät für beide WAN-Links dasselbe (der Switch) und nicht unterschiedlich (die Firewalls) wie im vorherigen Beispiel. Häufig wird dieses Verfahren angewendet, wenn sich die Firewall auf dem LAN im SD-WAN Edge befindet.



In dieser Topologie wird ein richtlinienbasiertes Routing verwendet, um Pakete auf den entsprechenden WAN-Link zu lenken. Diese Lenkung wird möglicherweise durch die IP-Adresse oder durch das VLAN-Tag durchgeführt. Daher unterstützen wir beide Optionen.

Lenkung über IP: Wenn das L3-Gerät in der Lage ist, richtlinienbasiertes Routing nach Quell-IP-Adresse durchzuführen, können sich beide Geräte im selben VLAN befinden. In diesem Fall ist lediglich eine benutzerdefinierte Quell-IP zur Unterscheidung der Geräte erforderlich.

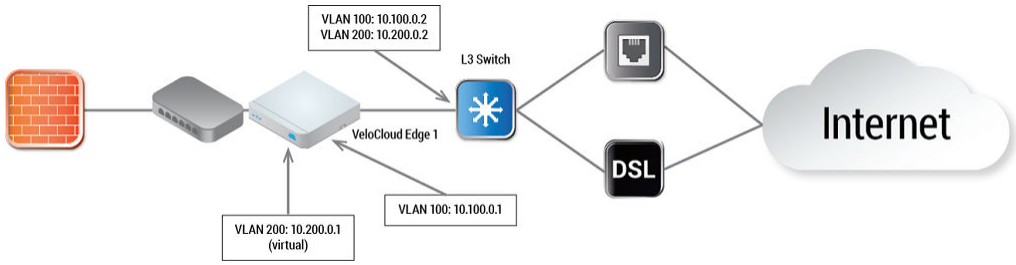


Im folgenden Abschnitt wird beschrieben, wie die endgültige Konfiguration definiert ist.

- Die Schnittstelle ist mit der IP-Adresse 10.0.0.1 und dem nächsten Hop 10.0.0.2 definiert. Da mehr als ein WAN-Link an die Schnittstelle angeschlossen ist, werden die Links auf „benutzerdefiniert (user defined)“ festgelegt.

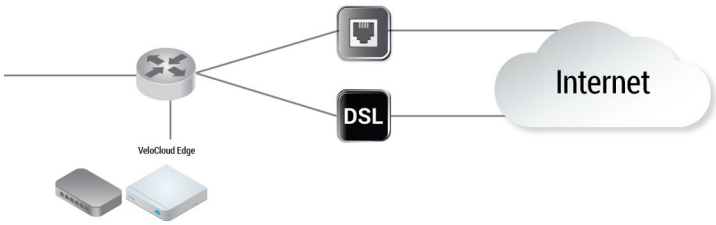
- Der Kabel-Link ist definiert und erbt die IP-Adresse von 10.0.0.1 und den nächsten Hop von 10.0.0.2. Es sind keine Änderungen erforderlich. Wenn ein Paket über den Kabel-Link gesendet werden muss, wird es von 10.0.0.1 bezogen und an das Gerät weitergeleitet, das auf ARP für 10.0.0.2 (L3-Switch) antwortet. Rückgabepakete sind für 10.0.0.1 bestimmt und werden als auf dem Kabel-Link ankommend erkannt.
- Der DSL-Link ist definiert, und da es sich um den zweiten WAN-Link handelt, kennzeichnet die SD-WAN Orchestrator-Instanz die IP-Adresse und den nächsten Hop als obligatorische Konfigurationselemente. Der Benutzer gibt eine benutzerdefinierte virtuelle IP (z. B. 10.0.0.3) für die Quell-IP und dieselbe 10.0.0.2-IP für den nächsten Hop an. Wenn ein Paket über den DSL-Link gesendet werden muss, wird es von 10.0.0.3 bezogen und an das Gerät weitergeleitet, das auf ARP für 10.0.0.2 (L3-Switch) antwortet. Rückgabepakete sind für 10.0.0.3 bestimmt und werden als auf dem DSL-Link ankommend erkannt.

Lenkung über VLAN: Wenn das L3-Gerät nicht in der Lage ist, das Quell-Routing durchzuführen, oder wenn der Benutzer aus einem anderen Grund beschließt, den Kabel- und DSL-Links separate VLANs zuzuweisen, muss dies konfiguriert werden.



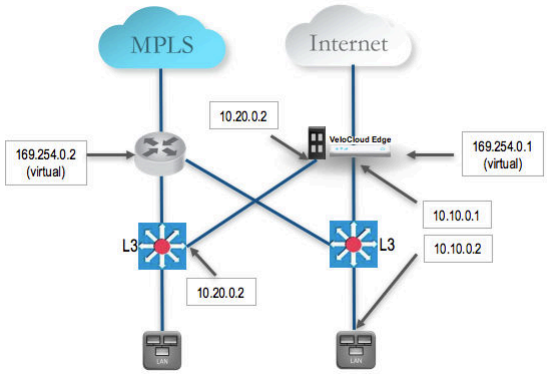
- Die Schnittstelle ist mit der IP-Adresse 10.100.0.1 und dem nächsten Hop 10.100.0.2 auf VLAN 100 definiert. Da mehr als ein WAN-Link an die Schnittstelle angeschlossen ist, werden die Links auf „benutzerdefiniert (user-defined)“ festgelegt.
- Der Kabel-Link ist definiert und erbt VLAN 100 sowie die IP-Adresse von 10.100.0.1 und den nächsten Hop von 10.100.0.2. Es sind keine Änderungen erforderlich. Wenn ein Paket über den Kabel-Link gesendet werden muss, wird es von 10.100.0.1 mit dem VLAN 100-Tag bezogen und an das Gerät weitergeleitet, das auf ARP für 10.100.0.2 auf VLAN 100 (L3-Switch) antwortet. Rückgabepakete sind für 10.100.0.1/VLAN 100 bestimmt und werden als auf dem Kabel-Link ankommend erkannt.
- Der DSL-Link ist definiert, und da es sich um den zweiten WAN-Link handelt, kennzeichnet die SD-WAN Orchestrator-Instanz die IP-Adresse und den nächsten Hop als obligatorische Konfigurationselemente. Der Benutzer gibt eine benutzerdefinierte VLAN-ID (200) sowie eine virtuelle IP (z. B. 10.200.0.1) für die quellseitige IP und die 10.200.0.2-IP für den nächsten Hop an. Wenn ein Paket über den DSL-Link gesendet werden muss, wird es von 10.200.0.1 mit dem VLAN 200-Tag bezogen und an das Gerät weitergeleitet, das auf ARP für 10.200.0.2 auf VLAN 200 (L3-Switch) antwortet. Rückgabepakete sind für 10.200.0.1/VLAN 200 bestimmt und werden als auf dem DSL-Link ankommend erkannt.

3 **Anwendungsfall 3: Einarmige Bereitstellungen**: Einarmige Bereitstellungen sind anderen L3-Bereitstellungen sehr ähnlich.



Auch hier teilt sich der SD-WAN Edge für beide WAN-Links den gleichen nächsten Hop. Ein richtlinienbasiertes Routing kann durchgeführt werden, um sicherzustellen, dass der Datenverkehr wie oben definiert an das entsprechende Ziel weitergeleitet wird. Alternativ können die IP-Adressen und das VLAN für die WAN-Link-Objekte im VMware SD-WAN mit dem VLAN der Kabel- und DSL-Links identisch sein, um das Routing automatisch durchzuführen.

4 **Anwendungsfall 4: Ein WAN-Link, der über mehrere Schnittstellen erreichbar ist**: Betrachten Sie die herkömmliche Gold-Site-Topologie, bei der das MPLS über zwei alternative Pfade erreichbar ist. In diesem Fall müssen Sie die IP-Adresse und den nächsten Hop einer benutzerdefinierten Quelle definieren, die unabhängig von der Schnittstelle, die für die Kommunikation verwendet wird, freigegeben werden kann.



- GE1 ist mit der IP-Adresse 10.10.0.1 und dem nächsten Hop 10.10.0.2 definiert.
- GE2 ist mit der IP-Adresse 10.20.0.1 und dem nächsten Hop 10.20.0.2 definiert.
- Das MPLS wird über eine der beiden Schnittstellen als erreichbar definiert und festgelegt. Dies macht die Quell-IP und die IP-Adresse des nächsten Hops ohne Voreinstellungen obligatorisch.
- Es werden die Quell-IP und das Ziel definiert, die unabhängig von der verwendeten Schnittstelle für die Kommunikation verwendet werden können. Wenn ein Paket über die

MPLS-Verbindung gesendet werden muss, wird es aus 169.254.0.1 bezogen, mit dem konfigurierten VLAN gekennzeichnet und an das Gerät weitergeleitet, das auf dem konfigurierten VLAN (CE-Router) auf ARP für 169.254.0.2 antwortet. Rückgabepakete sind für 169.254.0.1 bestimmt und werden als auf dem MPLS-Link ankommend erkannt.

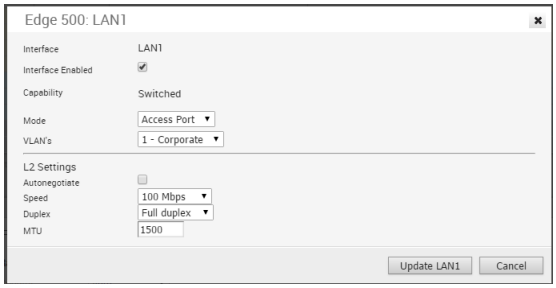
Hinweis Wenn OSPF oder BGP nicht aktiviert ist, müssen Sie möglicherweise ein Transit-VLAN konfigurieren, das auf beiden Switches dasselbe ist, um die Erreichbarkeit dieser virtuellen IP zu ermöglichen.

Schnittstellenkonfiguration

Wenn Sie auf den Link **Bearbeiten (Edit)** klicken, wird ein Dialogfeld für die Aktualisierung der Einstellungen für eine bestimmte Schnittstelle angezeigt. In den folgenden Abschnitten finden Sie eine kurze Beschreibung für die verschiedenen Dialogfelder, die für das Edge-Modell und die Schnittstellentypen vorgestellt werden.

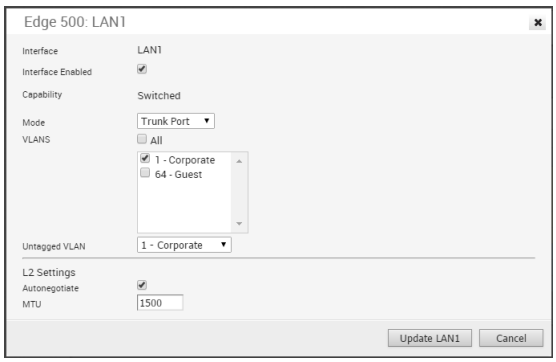
Edge 500-LAN-Zugriff

Im Folgenden werden die Parameter für eine Edge 500-LAN-Schnittstelle gezeigt, die als Zugriffsport konfiguriert ist. Sie können ein VLAN für den Anschluss auswählen und L2-Einstellungen für „Autom. aushandeln (Autonegotiate)“ (standardmäßig ausgewählt), „Geschwindigkeit (Speed)“, Duplex-Typ und MTU-Größe (Standardwert 1500) auswählen.



Edge 500-LAN-Trunk

Im Folgenden werden die Parameter für eine Edge 500-LAN-Schnittstelle gezeigt, die als Trunk-Port konfiguriert ist. Sie können VLANs für den Port auswählen, angeben, wie nicht markierte VLAN-Daten behandelt werden (an ein bestimmtes VLAN weitergeleitet oder gelöscht), und L2-Einstellungen für „Autom. aushandeln (Autonegotiate)“ (standardmäßig ausgewählt), „Geschwindigkeit“, „Duplex-Typ“ und „MTU-Größe“ (Standardwert 1500) auswählen.

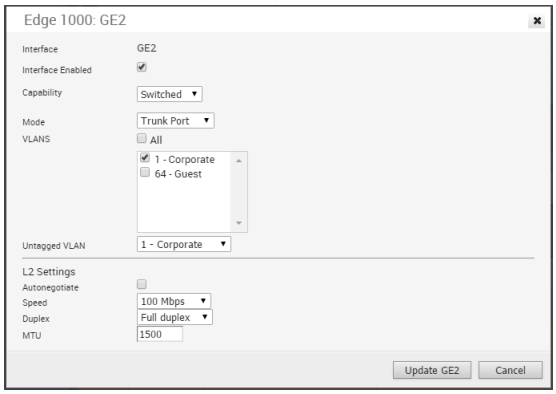


Edge 1000-LAN-Zugriff

Im Folgenden werden die Parameter für eine Edge 1000-LAN-Schnittstelle gezeigt, die als Switched Access Port konfiguriert ist. Sie können ein VLAN für den Anschluss auswählen und L2-Einstellungen für „Autom. aushandeln (Autonegotiate)“ (standardmäßig ausgewählt), „Geschwindigkeit (Speed)“, Duplex-Typ und MTU-Größe (Standardwert 1500) auswählen.

Edge 1000-LAN-Trunk

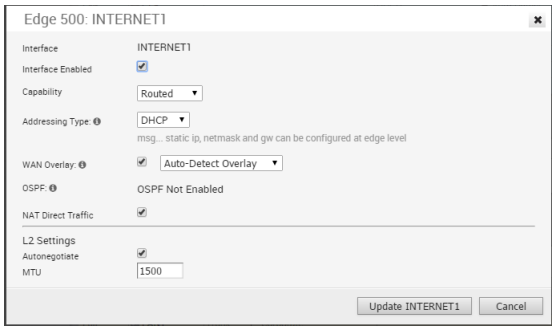
Im Folgenden werden die Parameter für eine Edge 1000-LAN-Schnittstelle gezeigt, die als Trunk-Port konfiguriert ist. Sie können VLANs für den Port auswählen, angeben, wie nicht markierte VLAN-Daten behandelt werden (an ein bestimmtes VLAN weitergeleitet oder gelöscht), und L2-Einstellungen für „Autom. aushandeln (Autonegotiate)“ (standardmäßig ausgewählt), „Geschwindigkeit“, „Duplex-Typ“ und „MTU-Größe“ (Standardwert 1500) auswählen.



Edge 500-WAN

Im Folgenden werden die Parameter für eine Edge 500-WAN-Schnittstelle mit der Funktion „Weitergeleitet (Routed)“ gezeigt. Sie können den Adresstyp (DHCP, PPPoE oder statisch) und ein WAN-Overlay (automatische Erkennung oder benutzerdefiniert) auswählen, OSPF aktivieren, NAT Direct-Datenverkehr aktivieren und L2-Einstellungen für „Autom. aushandeln (Autonegotiate)“ (standardmäßig ausgewählt), „Geschwindigkeit (Speed)“, Duplex-Typ und MTU-Größe (Standardwert 1500) auswählen.

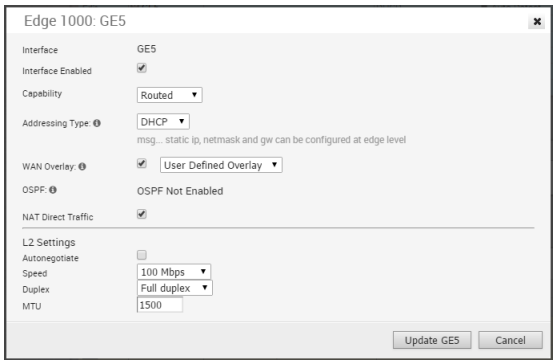
Hinweis Der Port kann auch als eine Switched-Schnittstelle konfiguriert werden.



Edge 1000-WAN

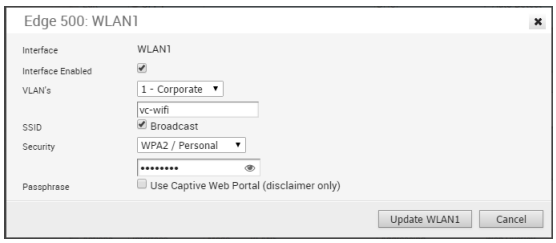
Im Folgenden werden die Parameter für eine Edge 1000-WAN-Schnittstelle mit der Funktion **Weitergeleitet (Routed)** gezeigt. Sie können den Adresstyp (DHCP, PPPoE oder statisch) und ein WAN-Overlay (automatische Erkennung oder benutzerdefiniert) auswählen, OSPF aktivieren, NAT Direct-Datenverkehr aktivieren und L2-Einstellungen für „Autom. aushandeln (Autonegotiate)“ (standardmäßig ausgewählt), „Geschwindigkeit (Speed)“, Duplex-Typ und MTU-Größe (Standardwert 1500) auswählen.

Hinweis Der Port kann auch als eine Switched-Schnittstelle konfiguriert werden.



Edge 500-WLAN

Anfänglich sind zwei WLAN-Netzwerke für den SD-WAN Edge 500 definiert, eines als Unternehmensnetzwerk und eines als Gastnetzwerk, das anfänglich deaktiviert ist. Es können zusätzliche drahtlose Netzwerke definiert werden, jedes mit einer spezifischen VLAN-, SSID- und Sicherheitskonfiguration.



Sicherheit für WLAN-Verbindungen

Ihre WLAN-Verbindungen können wie folgt gesichert werden:

Typ	Beschreibung
Offen (Open)	Es wird keine Sicherheit erzwungen.
WPA2 / Persönlich (WPA2 / Personal)	Zum Authentifizieren eines Benutzers wird ein Kennwort verwendet.
WPA2 / Unternehmen (WPA2 / Enterprise)	Zum Authentifizieren eines Benutzers wird ein Radius-Server verwendet. In diesem Szenario muss ein Radius-Server unter „Netzwerkdienste (Network Services)“ konfiguriert und „Radius-Server (Radius Server)“ muss in den **Profilauthentifizierungseinstellungen (Profile Authentication Settings)** auf der Seite **Gerät (Device)** ausgewählt werden. Die Standardeinstellungen für die Sicherheit können auch auf der Seite **Edge-Gerät (Edge Device)** außer Kraft gesetzt werden.

Konfigurieren von WLAN-Funkeinstellungen

Auf der Profilebene können Sie den WLAN-Funk aktivieren/deaktivieren und den Funkfrequenzbereich konfigurieren.

Verfahren

1 Klicken Sie im Unternehmensportal auf **Konfigurieren (Configure)** > **Profile (Profiles)**.

Die Seite **Konfigurationsprofile (Configuration Profiles)** wird angezeigt.

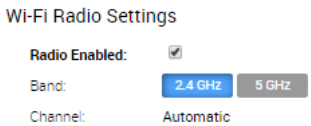
2 Wählen Sie ein Profil aus, für das Sie die WLAN-Funkeinstellungen konfigurieren möchten, und klicken Sie auf das Symbol unter der Spalte **Gerät (Device)**.

Die Seite **Geräteeinstellungen (Device Settings)** wird für das ausgewählte Profil angezeigt.

3 Im Bereich **WLAN-Funkeinstellungen (WI-FI Radio Settings)** ist das Kontrollkästchen **Funk aktiviert (Radio Enabled)** standardmäßig aktiviert, und der **Kanal (Channel)** ist auf **Automatisch (Automatic)** festgelegt.

4 Wählen Sie den Funkbereich aus. Der Wert kann **2,4 GHz** oder **5 GHz** lauten.

5 Klicken Sie auf **Änderungen speichern (Save Changes)**.



Auf der Edge-Ebene können Sie die im Profil angegebenen WLAN-Einstellungen außer Kraft setzen, indem Sie das Kontrollkästchen **Edge-Außerkraftsetzung aktivieren (Enable Edge Override)** aktivieren. Weitere Informationen finden Sie unter Konfigurieren von Außerkraftsetzungen für WLAN-Funk.

Konfigurieren von SNMP-Einstellungen auf der Profilebene

SNMP ist ein häufig verwendetes Protokoll für die Netzwerküberwachung, und MIB ist eine Datenbank, die SNMP zur Verwaltung von Entitäten zugeordnet ist. SNMP kann aktiviert werden, indem Sie die gewünschte SNMP-Version auswählen, wie in den Schritten unten erläutert.

Bevor Sie beginnen:

- So laden Sie die SD-WAN Edge-MIB herunter: Navigieren Sie zum Bildschirm **Remote-Diagnose (Remote Diagnostic)** (**Testen und Fehlerbehebung > Remote-Diagnose (Test & Troubleshooting > Remote Diagnostics)**) und führen Sie MIB für SD-WAN Edge aus. Kopieren und Einfügen von Ergebnissen auf Ihre lokale Maschine.
- Installieren Sie alle von VELOCLOUD-EDGE-MIB benötigten MIBs auf dem Client-Host, einschließlich SNMPv2-SMI, SNMPv2-CONF, SNMPv2-TC, INET-ADDRESS-MIB, IF-MIB, UUID-TC-MIB und VELOCLOUD-MIB. Alle oben genannten MIBs, außer VELOCLOUD-MIB, können online gefunden werden. Überprüfen Sie für VELOCLOUD-MIB die VeloCloud-Website.

Unterstützte MIBs

- SNMP MIB-2-System
- SNMP MIB-2-Schnittstellen
- VELOCLOUD-EDGE-MIB
- HOST-RESOURCES-MIB, von RFC 1514

Vorgehensweise zum Konfigurieren von SNMP-Einstellungen auf der Profilebene:

1 Rufen Sie die VELOCLOUD-EDGE-MIB über **Remote-Diagnose (Remote Diagnostic)** ab.

2 Installieren Sie alle MIBs, die von VELOCLOUD-EDGE-MIB benötigt werden. (Weitere Informationen finden Sie unter „Bevor Sie beginnen“.)

3 Navigieren Sie in SD-WAN Orchestrator zu **Konfigurieren (Configure) > Profile (Profiles)**.

Der Bildschirm **Konfigurationsprofile (Configuration Profiles)** wird angezeigt.

4 Wählen Sie ein Profil aus, für das Sie SNMP-Einstellungen konfigurieren möchten, und klicken Sie auf das Symbol **Gerät (Device)** in der Spalte „Gerät (Device)“.

Der Bildschirm **Konfigurationsprofile (Configuration Profiles)** für das ausgewählte Profil wird angezeigt.

5 Scrollen Sie nach unten bis zum Bereich **SNMP-Einstellungen (SNMP Settings)**. Sie können zwischen zwei Versionen wählen: v2c oder v3.

6 Führen Sie für eine SNMP v2c-Konfiguration die folgenden Schritte aus:

a Aktivieren Sie das Kontrollkästchen **v2c**.

b Geben Sie einen Port in das Textfeld **Port** ein. Die Standardeinstellung ist 161.

c Geben Sie im Textfeld **Community** ein Wort oder eine Zahlenfolge ein, die als „Kennwort“ fungiert und Ihnen den Zugriff auf den SNMP-Agenten ermöglicht.

d Für zulässige IPs:

- Aktivieren Sie das Kontrollkästchen **Alle (Any)**, damit jede IP-Adresse auf den SNMP-Agenten zugreifen kann.
- Um den Zugriff auf den SNMP-Agenten einzuschränken, deaktivieren Sie das Kontrollkästchen **Alle (Any)** und geben Sie die IP-Adresse(n) ein, die für den Zugriff auf den SNMP-Agenten zulässig ist/sind.

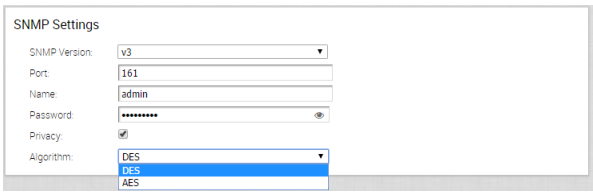
7 Führen Sie für eine SNMP v3-Konfiguration, die zusätzliche Sicherheitsunterstützung bietet, die folgenden Schritte aus:

a Geben Sie einen Port in das Textfeld **Port** ein. Die Standardeinstellung ist 161.

b Geben Sie einen Benutzernamen und ein Kennwort in die entsprechenden Textfelder ein.

c Aktivieren Sie das Kontrollkästchen **Datenschutz (Privacy)**, wenn Sie die Paketübertragung verschlüsseln möchten.

d Wenn Sie das Kontrollkästchen **Datenschutz (Privacy)** aktiviert haben, wählen Sie aus dem Dropdown-Menü **Algorithmus (Algorithm)** „DES“ oder „AES“ aus.



8 Konfigurieren Sie die Firewalleinstellungen. Nachdem Sie SNMP-Einstellungen konfiguriert haben, navigieren Sie zu den Firewalleinstellungen (**Konfigurieren >Profile > Firewall (Configure >Profiles > Firewall)**), um die Firewalleinstellungen zu konfigurieren, die Ihre SNMP-Einstellungen aktivieren.

Hinweis Die Überwachung der SNMP-Schnittstelle wird auf DPDK-fähigen Schnittstellen der Version 3.3.0 und höher unterstützt.

Konfigurieren des Sichtbarkeitsmodus

In diesem Abschnitt wird beschrieben, wie Sie den Sichtbarkeitsmodus konfigurieren.

Informationen zum Sichtbarkeitsmodus

Obwohl die Nachverfolgung anhand der MAC-Adresse ideal ist (Bereitstellung einer globalen, eindeutigen Kennung), besteht ein Mangel an Transparenz, wenn sich ein L3-Switch zwischen dem Client und dem Edge befindet, da die Switch-MAC dem Edge bekannt ist, nicht die Geräte-MAC. Aus diesem Grund sind zwei Nachverfolgungsmodi (MAC-Adresse und jetzt IP-Adresse) verfügbar. Wenn die Verfolgung nach MAC-Adresse nicht möglich ist, wird stattdessen die IP-Adresse verwendet.

Auswählen des Sichtbarkeitsmodus

Um einen **Sichtbarkeitsmodus (Visibility Mode)** auszuwählen, navigieren Sie zu **Konfigurieren > Profil > Geräte (Configure > Profile > Devices)**. Wählen Sie eine der folgenden Optionen aus:

- **Sichtbarkeit nach MAC-Adresse (Visibility by MAC address)**
- **Sichtbarkeit nach IP-Adresse (Visibility by IP address)**

Überlegungen zur Verwendung des Sichtbarkeitsmodus

Beachten Sie bei der Auswahl eines Sichtbarkeitsmodus Folgendes:

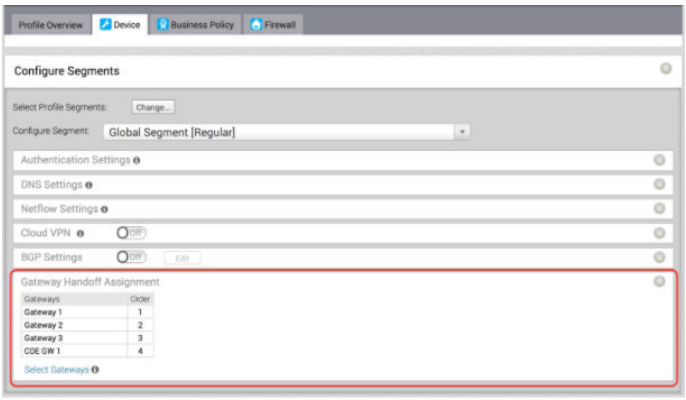
- Wenn **Sichtbarkeit nach MAC-Adresse (Visibility by MAC address)** ausgewählt ist:
  - Clients befinden sich hinter L2 SW
  - Client-MAC, IP und Hostname werden (ggf.) angezeigt
  - Statistiken werden basierend auf MAC erfasst
- Wenn **Sichtbarkeit nach IP-Adresse (Visibility by IP address)** ausgewählt ist:
  - Clients befinden sich hinter L3 SW
  - SW MAC, Client-IP und Hostname werden (ggf.) angezeigt.
  - Statistiken werden basierend auf der IP erfasst

Zuweisen von Partner-Gateways

Damit Kunden Partner-Gateways nutzen können, muss Ihr Operator das Kontrollkästchen **Übergabe an Partner aktivieren (Enable Partner Handoff)** für das Gateway aktivieren, um diese Funktion zu aktivieren. Wenn Ihnen diese Funktion zur Verfügung steht, wird der Bereich

Zuweisung von Partner-Gateways (Partner Gateway Assignment) auf der Registerkarte **Konfigurieren > Profile > Gerät (Configure > Profiles > Device)** angezeigt.

Hinweis Die Funktion „Zuweisung von Partner-Gateways“ (Partner Gateway Assignment) wurde verbessert und unterstützt jetzt segmentbasierte Konfigurationen. Mehrere Partner-Gateways können auf der Profilebene konfiguriert und/oder auf der Edge-Ebene außer Kraft gesetzt werden.



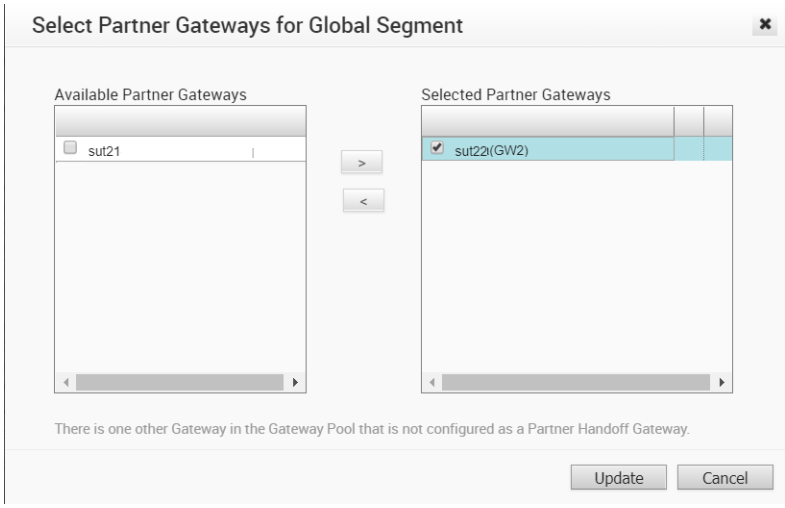
Gateways auswählen

Um die Schritte in diesem Abschnitt auszuführen, muss diese Funktion aktiviert sein. Weitere Informationen erhalten Sie bei Ihrem Operator.

Wenn im Bereich **Zuweisung der Gateway-Übergabe (Gateway Handoff Assignment)** keine Gateways aufgelistet sind:

1 Klicken Sie auf den Link **Gateways auswählen (Select Gateways)**, um Partner-Gateways auszuwählen.

2 Wählen Sie im Dialogfeld **Partner-Gateways für globales Segment auswählen (Select Partner Gateways for Global Segment)** im Bereich **Verfügbares Partner-Gateway (Available Partner Gateway)** ein verfügbares Partner-Gateway aus und verschieben Sie es (mit dem entsprechenden Pfeil) in den Bereich **Ausgewähltes Partner-Gateway (Selected Partner Gateway)**.



Beachten Sie, dass nur Gateways, die als Partner-Übergabe-Gateway konfiguriert sind, im Bereich **Verfügbare Partner-Gateways (Available Partner Gateways)** angezeigt werden. Wenn andere Gateways nicht als Partner-Übergabe-Gateway konfiguriert sind, wird die folgende Meldung im Dialogfeld angezeigt: **Im Gateway-Pool befindet sich ein anderes Gateway, das nicht als Partner-Übergabe-Gateway konfiguriert ist (There is one other Gateway in the Gateway Pool that is not configured as a Partner Handoff Gateway)**.

Auswählen von CDE-Gateways

In normalen Szenarien fließt der PCI-Datenverkehr zwischen der Kundenfiliale und dem Datencenter, wobei der PCI-Datenverkehr an das PCI-Netzwerk weitergeleitet wird und die Gateways außerhalb des PCI-Bereichs liegen. (Der Operator kann das Gateway so konfigurieren, dass das PCI-Segment ausgeschlossen wird, indem die CDE-Rolle deaktiviert wird.)

In bestimmten Szenarien, in denen Gateways eine Übergabe an das PCI-Netzwerk und im PCI-Bereich haben können, kann der Operator die CDE-Rolle für die Partner-Gateways aktivieren. Diese Gateways (CDE-Gateways) stehen dem Benutzer dann zur Zuweisung in den PCI-Segmenten (CDE-Typ) zur Verfügung.

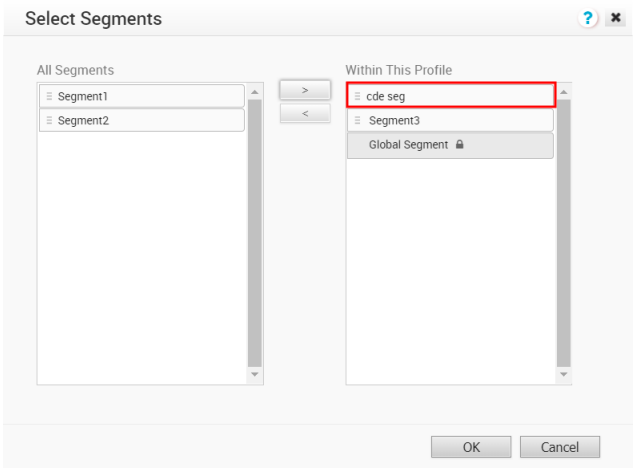
Um die Schritte in diesem Abschnitt auszuführen, muss diese Funktion aktiviert sein. Weitere Informationen erhalten Sie bei Ihrem Operator.

Zuweisen eines CDE-Gateways

So weisen Sie ein CDE-Gateway zu:

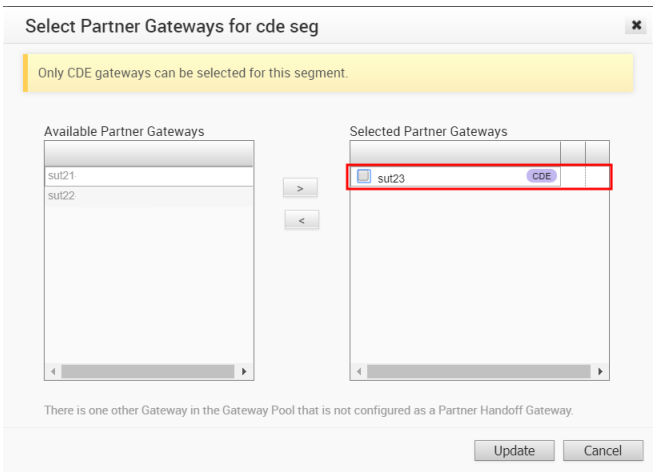
1 Klicken Sie im Fenster **Segmente konfigurieren (Configure Segments)** auf die Schaltfläche **Profilsegmente auswählen (Select Profile Segments)** und dann auf **Ändern (Change)**.

2 Verschieben Sie im Dialogfeld **Segmente auswählen (Select Segments)** das verfügbare CDE-Segment aus dem Bereich **Verfügbare Segmente (Available Segments)** (mit dem entsprechenden Pfeil) in den Bereich **In diesem Profil (Within This Profile)**.



3 Klicken Sie im Bereich **Zuweisung der Gateway-Übergabe (Gateway Handoff Assignment)** auf den Link **Gateways auswählen (Select Gateways)**.

4 Wählen Sie im Bereich **Partner-Gateways für CDE-Segment auswählen (Select Partner Gateways for cde seg)** ein verfügbares CDE-Partner-Gateway (im Bereich **Verfügbare Partner-Gateways (Available Partner Gateways)**) aus und verschieben Sie es in den Bereich **Ausgewählte Partner-Gateways (Selected Partner Gateways)**.



5 Klicken Sie auf die Schaltfläche **Aktualisieren (Update)**.

Der Bereich **Zuweisung der Gateway-Übergabe (Gateway Handoff Assignment)** wird mit den ausgewählten Gateways aktualisiert.

Hinweis Wie im Dialogfeld **Partner-Gateways für CDE-Segment auswählen (Select Partner Gateways for cde seg)** angegeben, können nur CDE-Gateways für das Segment ausgewählt werden.

Überlegungen beim Zuweisen von Partner-Gateways:

Beachten Sie die folgenden Hinweise beim Zuweisen von Partner-Gateways:

- Partner-Gateways können auf Profil- oder Edge-Ebene zugewiesen werden.
- Einem Edge können mehr als zwei Partner-Gateways (bis zu 16) zugewiesen werden.
- Partner-Gateways können per Segment zugewiesen werden.

Hinweis Wenn der Bereich **Zuweisung der Gateway-Übergabe (Gateway Handoff Assignment)** im Fenster **Segmente konfigurieren (Configure Segments)** nicht angezeigt wird, bitten Sie Ihren Operator, diese Funktion zu aktivieren.

Zuweisen von Controllern

Das SD-WAN Gateway ist für die Unterstützung der Daten- und Steuerungsebene aktiviert. In Version 3.2 führt VMware SD-WAN eine reine Controller-Funktion (Controller-Gatewayzuweisung) ein.

Es gibt mehrere Anwendungsfälle, in denen das SD-WAN Gateway nur als Controller fungieren muss (d. h., um die Funktionen der Datenebene zu entfernen). Darüber hinaus ermöglicht dies dem Gateway eine unterschiedliche Skalierung, da Ressourcen, die normalerweise für die Paketverarbeitung vorgesehen sind, zur Unterstützung der Verarbeitung auf der Steuerungsebene verschoben werden können. Dies ermöglicht beispielsweise die Unterstützung einer höheren Anzahl gleichzeitiger Tunnel auf einem Controller als auf einem herkömmlichen Gateway. Im folgenden Abschnitt finden Sie einen typischen Anwendungsfall.

Anwendungsfall: Dynamische Weiterleitung von Zweigstelle zu Zweigstelle über verschiedene Partner-Gateways

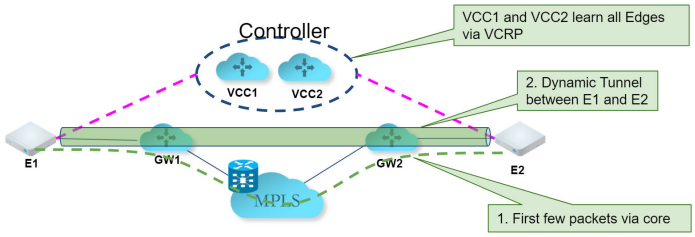
In diesem Szenario gehören Edge 1 (E1) und Edge 2 (E2), wie in der Abbildung gezeigt, zu demselben Unternehmen in der Orchestrator-Instanz. Allerdings stellen Sie eine Verbindung zu unterschiedlichen Partnergateways (in der Regel in unterschiedlichen Regionen) her. Aus diesem Grund ist eine dynamische Zweigstelle zwischen E1 und E2 nicht möglich, aber durch die Nutzung des Controllers ist dies möglich.

Anfänglicher Datenverkehrsfluss

Wie in der Abbildung unten gezeigt, beginnt der Datenverkehrsfluss, wenn E1 und E2 versuchen, direkt zu kommunizieren, wie in früheren Versionen des Codes durch das private Netzwerk zu laufen. Gleichzeitig benachrichtigen die Edges auch den Controller, dass sie kommunizieren, und fordern eine direkte Verbindung an.

Dynamischer Tunnel

Der Controller signalisiert den Edges, den dynamischen Tunnel zu erstellen, indem er E1-Konnektivitätsinformationen für E2 und umgekehrt bereitstellt. Der Verkehrsfluss geht nahtlos in den neuen dynamischen Tunnel über, falls und sobald dieser erstellt wird.



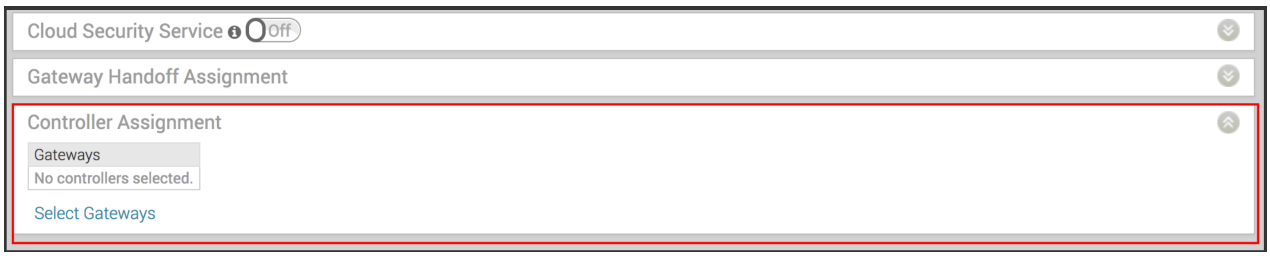
Konfigurieren eines Gateways als Controller

Damit Kunden Partner-Gateways nutzen können, muss Ihr Operator das Kontrollkästchen **Übergabe an Partner aktivieren (Enable Partner Handoff)** für das Gateway aktivieren, um diese Funktion zu aktivieren. Wenn Ihnen diese Funktion zur Verfügung steht, wird der Bereich **Controller-Zuweisung (Controller Assignment)** auf der Registerkarte **Konfigurieren > Profile > Gerät (Configure > Profiles > Device)** des Bildschirms angezeigt.

Hinweis Mindestens ein Gateway im Gateway-Pool sollte ein „Nur Controller"-Gateway sein.

1 Navigieren Sie zur Registerkarte **Konfigurieren > Profile > Gerät (Configure > Profiles > Device)**.

2 Scrollen Sie nach unten zum Bereich **Controller-Zuweisung (Controller Assignment)**.



3 Klicken Sie im Bereich **Controller-Zuweisung (Controller Assignment)** auf den Link **Gateways auswählen (Select Gateways)**.

4 Verschieben Sie im Dialogfeld **Controller für globales Segment auswählen (Select Controllers for Global Segment)** die Controller aus dem Bereich **Verfügbar (Available)** in den Bereich **Ausgewählt (Selected)**.

5 Klicken Sie auf **Aktualisieren (Update)**.

Der Bereich **Controller-Zuweisung (Controller Assignment)** wird aktualisiert.

Konfigurieren der Unternehmensrichtlinie für ein Profil

11

VMware SD-WAN bietet eine Funktion für erweiterte QoS-Funktion namens „Unternehmensrichtlinie“. Diese Funktion wird mithilfe der Registerkarte **Unternehmensrichtlinie (Business Policy)** in einem Profil oder auf der Ebene der Profil- oder Edge-Überschreibung definiert.

Hinweis Wenn Sie mit einer Benutzer-ID angemeldet sind, die über Kundensupport-Berechtigungen verfügt, können Sie nur SD-WAN Orchestrator-Objekte anzeigen. Sie werden nicht in der Lage sein, neue Objekte zu erstellen oder bestehende zu konfigurieren/aktualisieren.

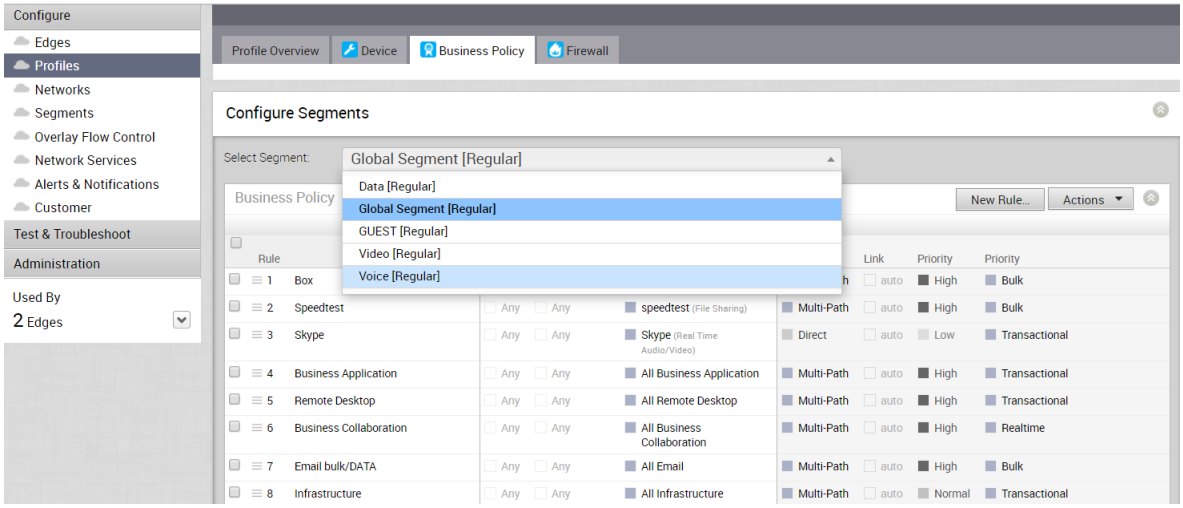
Basierend auf der Konfiguration der Unternehmensrichtlinie untersucht VMware SD-WAN den verwendeten Datenverkehr, identifiziert das Anwendungsverhalten, das für eine bestimmte Anwendung erforderliche Unternehmensdienstziel (hoch, mittel oder niedrig) und die Bedingungen der Edge-WAN-Verbindung. Auf dieser Grundlage optimiert die Unternehmensrichtlinie das Anwendungsverhalten, das die Warteschlangenbildung, die Bandbreitennutzung, die Verbindungssteuerung und die Minderung von Netzwerkfehlern vorantreibt.

Die nachstehende Bildschirmaufnahme zeigt einige der Regeln der Unternehmensrichtlinie. Eine Reihe von Regeln ist vordefiniert, und Sie können Ihre eigenen Regeln hinzufügen, um Ihren Netzwerkbetrieb anzupassen. Die Regeln sind in der Reihenfolge ihrer höchsten Priorität aufgeführt. Der Netzwerkverkehr wird verwaltet, indem seine Merkmale identifiziert und dann die Merkmale der Regel mit der höchsten Priorität zugeordnet werden.

Wie in der Abbildung unten gezeigt, sind die Regeln der Unternehmensrichtlinie jetzt segmentierfähig. Alle für die Konfiguration verfügbaren Segmente werden im Dropdown-Menü **Segment konfigurieren (Configure Segment)** aufgelistet.

Wenn Sie ein zu konfigurierendes Segment aus dem Dropdown-Menü**Segment konfigurieren (Configure Segment)** auswählen, werden die mit diesem Segment verbundenen Einstellungen und Optionen im Bereich **Segmente konfigurieren (Configure Segments)** angezeigt. **Globales Segment [Normal] (Global Segment [Regular])** ist das Standardsegment.

Weitere Informationen zur Segmentierung finden Sie unter Kapitel 7 Konfigurieren von Segmenten und Kapitel 10 Konfigurieren eines Profilgeräts.



Hinweis Sie können Ihre konfigurierten Regeln in der Liste der Regeln nach oben oder unten verschieben, um die Priorität festzulegen, indem Sie den Mauszeiger über den numerischen Wert auf der linken Seite der Regel bewegen und die Regel nach oben oder unten verschieben. Wenn Sie den Mauszeiger über die rechte Seite einer Regel bewegen, klicken Sie auf das **Minuszeichen (-)** neben der Regel, um sie aus der Liste zu entfernen, oder auf das **Pluszeichen (+)**, um eine neue Regel hinzuzufügen.

Dieses Kapitel enthält die folgenden Themen:

Erstellen einer Unternehmensrichtlinie

Operatoren, Partner und Administratoren auf allen Ebenen können eine Unternehmensrichtlinie erstellen.

Bevor Sie beginnen: Informieren Sie sich über die IP-Adressen Ihrer Geräte und die Auswirkungen der Einstellung einer Platzhaltermaske.

Über diese Aufgabe (About this task): Drei neue Optionen für IP-Adressen stehen zur Verfügung: **CIDR-Präfix (CIDR Prefix)**, **Subnetzmaske (Subnet Mask)** und **Platzhaltermaske (Wildcard Mask)**.

So erstellen Sie eine Unternehmensrichtlinie:

1 Klicken Sie auf **Neue Regel (New Rule)**, um eine Regel für die Unternehmensrichtlinie hinzuzufügen.

   Das Dialogfeld **Regel konfigurieren (Configure Rule)** wird angezeigt.

2 Im Bereich **Übereinstimmung (Match)** des Dialogfelds **Regel konfigurieren (Configure Rule)** werden drei Abschnitte für die Konfiguration des Datenverkehrs angezeigt:

   - **Quelle (Source)**
   - **Ziel (Destination)**

- **Anwendung (Application)**

Weitere Informationen zum Konfigurieren des Abschnitts **Quelle (Source)** im Bereich **Übereinstimmung (Match)** finden Sie in den folgenden Schritten.

3 Klicken Sie im Abschnitt **Quelle (Source)** auf die Schaltfläche **Definieren (Define)**, wenn Sie den Quelldatenverkehr auf ein bestimmtes VLAN, eine IP-Adresse oder ein Betriebssystem eingrenzen möchten. Standardmäßig ist die Schaltfläche **Alle (Any)** ausgewählt.

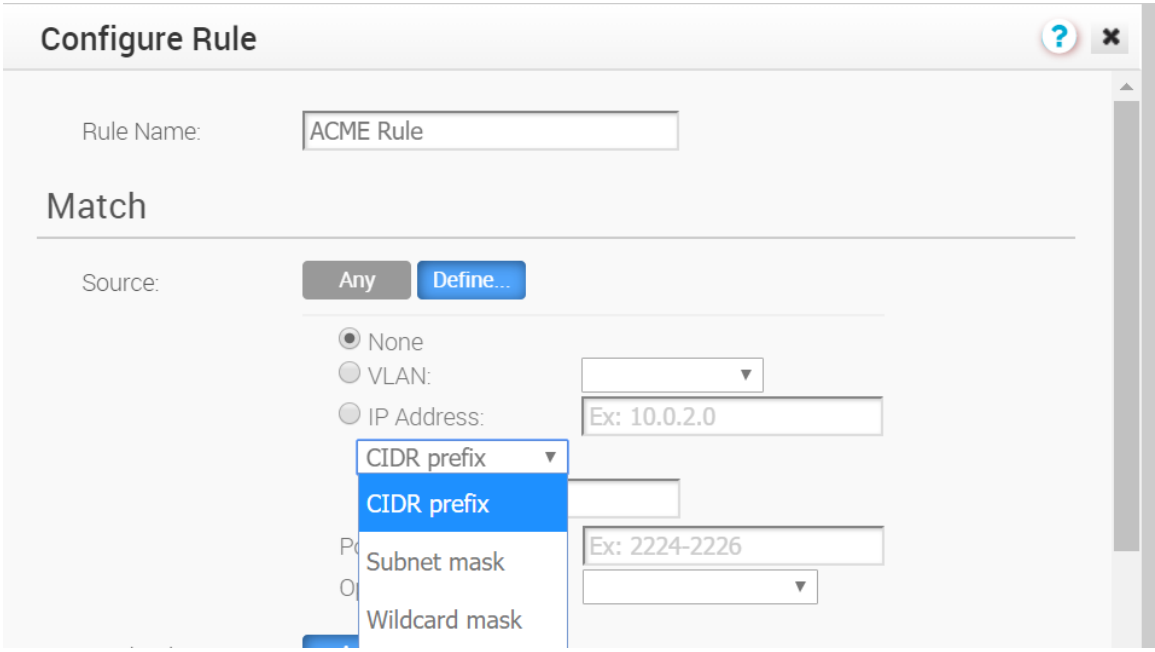
4 Wenn Sie auf die Schaltfläche **Definieren (Define)** klicken, wählen Sie die entsprechenden Optionen in den unten aufgeführten Schritten aus.

a **Keine (None)**: Standardmäßig ausgewählt.

b **VLAN**: Klicken Sie auf das Optionsfeld **VLAN** und wählen Sie das entsprechende VLAN aus dem Dropdown-Menü aus.

c **IP-Adresse (IP Address)**: Klicken Sie auf **IP-Adresse (IP Address)** und geben Sie die IP-Adresse ein. Wählen Sie dann eine der drei Optionen im Dropdown-Menü „CIDR-Präfix (CIDR Prefix)“, „Subnetzmaske (Subnet Mask)“ oder „Platzhaltermaske (Wildcard Mask)“ aus.

Option	Beschreibung
CIDR-Präfix (CIDR Prefix)	Wählen Sie diese Option aus, wenn das Netzwerk als Wert für CIDR definiert werden soll (z. B. `172.10.0.0 /16`).
Subnetzmaske (Subnet Mask)	Wählen Sie diese Option aus, wenn das Netzwerk basierend auf einer Subnetzmaske definiert werden soll (z. B. `172.10.0.0 255.255.0.0`).
Platzhaltermaske (Wildcard Mask)	Wählen Sie die Option „Platzhaltermaske (Wildcard Mask)“ aus, wenn Sie die Durchsetzung einer Richtlinie auf eine Reihe von Geräten für verschiedene IP-Subnetze beschränken möchten, die einen übereinstimmenden Wert für die IP-Adresse des Hosts verwenden. Die Platzhaltermaske entspricht einer IP oder einer Reihe von IP-Adressen, die auf der umgekehrten Subnetzmaske basieren. Eine 0 innerhalb des Binärwerts der Maske bedeutet, dass der Wert „fest“ ist, und eine 1 innerhalb des Binärwerts der Maske bedeutet, dass der Wert „variabel“ ist (kann 1 oder 0 sein). Beispiel: eine Platzhaltermaske von 0.0.0.255 (binäres Äquivalent = 00000000.00000000.00000000.11111111) mit einer IP-Adresse von 172.0.0, wobei die ersten drei Oktette feste Werte sind und das letzte Oktett ein variabler Wert ist. Hinweis: Nachdem Sie diese Regel mit einer Platzhaltermaske eingerichtet haben, schränken Sie die Anzahl der Clients ein, für die diese Regel gilt.



d **Ports**: Geben Sie die Ports in das entsprechende Textfeld ein.

e **Betriebssystem (Operating System)**: Wählen Sie im Dropdown-Menü das Betriebssystem des Clientgeräts aus.

5 Im Abschnitt **Ziel (Destination)** können Sie zusätzliche Parameter zuweisen, um das Datenverkehrsziel zu identifizieren, wie in den folgenden Schritten gezeigt:

a Definieren Sie Ihr Datenverkehrsziel, indem Sie auf eine der folgenden Optionen klicken: **Alle (Any)**, **Internet**, **VeloCloud-Edge (VeloCloud Edge)** oder **Nicht-VeloCloud-Site (Non-VeloCloud Site)**. Eine Beschreibung dieser Datenverkehrsziele finden Sie unter Konfigurieren des Übereinstimmungsziels. Hinweis: Das Zweigstelle-zu-Zweigstelle-Cloud-VPN muss aktiviert werden, bevor Sie Ihr Datenverkehrsziel definieren können.

b Geben Sie die IP-Adresse in das entsprechende Textfeld ein und geben Sie die Option „IP-Adresse (IP Address)“ an: **CIDR-Präfix (CIDR Prefix)**, **Platzhaltermaske (Wildcard mask)** und **Subnetzmaske (Subnet mask)**.

Option	Beschreibung
CIDR-Präfix (CIDR Prefix)	Wählen Sie diese Option aus, wenn das Netzwerk als Wert für CIDR definiert werden soll (z. B. `172.10.0.0 /16`).
Subnetzmaske (Subnet Mask)	Wählen Sie diese Option aus, wenn das Netzwerk basierend auf einer Subnetzmaske definiert werden soll (z. B. `172.10.0.0 255.255.0.0`).
Platzhaltermaske (Wildcard Mask)	Wählen Sie die Option „Platzhaltermaske (Wildcard Mask)“ aus, wenn Sie die Durchsetzung einer Richtlinie auf eine Reihe von Geräten für verschiedene IP-Subnetze beschränken möchten, die einen übereinstimmenden Wert für die IP-Adresse des Hosts verwenden. Die Platzhaltermaske entspricht einer IP oder einer Reihe von IP-Adressen, die auf der umgekehrten Subnetzmaske basieren. Eine 0 innerhalb des Binärwerts der Maske bedeutet, dass der Wert „fest“ ist, und eine 1 innerhalb des Binärwerts der Maske bedeutet, dass der Wert „variabel“ ist (kann 1 oder 0 sein). Beispiel: eine Platzhaltermaske von 0.0.0.255 (binäres Äquivalent = 00000000.00000000.00000000.11111111) mit einer IP-Adresse von 172.0.0, wobei die ersten drei Oktette feste Werte sind und das letzte Oktett ein variabler Wert ist. **Hinweis** Nachdem Sie diese Regel mithilfe einer Platzhaltermaske eingerichtet haben, verringern Sie die Anzahl der Clients, für die diese Regel gilt.

c **Hostnamen eingeben (Enter a Hostname)**: Verwenden Sie dieses Feld, um den gesamten Hostnamen oder einen Teil des Hostnamens abzugleichen. Zum Beispiel wird „salesforce“ den Datenverkehr mit „www.salesforce.com“ abgleichen.

d **Protokoll (Protocol)**: Ein Protokoll ist ein Satz von Regeln und Standards, die eine Sprache definieren, die Geräte zur Kommunikation verwenden. Wählen Sie ein Protokoll aus dem Dropdown-Menü (**GRE**, **ICMP**, **TCP** oder **UDP**) aus.

e **Ports**: Ein Port ist eine Adresse auf einem einzelnen Computer, die Sie mit einer bestimmten Software verbinden können. Geben Sie die entsprechende Portnummer in das Textfeld „Port“ ein.

6 Wählen Sie die Anwendungen im Abschnitt **Anwendung (Application)** aus:

a Klicken Sie auf die Schaltfläche **Definieren (Define)**, wenn Sie bestimmte Anwendungen auswählen möchten. Standardmäßig ist die Schaltfläche **Alle (Any)** ausgewählt.

b Wählen Sie in der Liste **Durchsuchen (Browse)** eine Anwendungskategorie aus. Eine bestimmte Anwendung, die auf der rechten Seite der Liste **Durchsuchen (Browse)** angezeigt wird. Scrollen Sie nach unten und wählen Sie die spezifische Anwendung aus, die Sie definieren möchten.

c Wählen Sie ein DSCP aus dem Dropdown-Menü aus.

7 Führen Sie im Bereich **Aktionen (Actions)** die folgenden Teilschritte aus:

a **Priorität (Priority)**: Legen Sie die Priorität der Regel fest (**Hoch (High)**, **Normal** oder **Niedrig (Low)**). Aktivieren Sie das Kontrollkästchen **Grenzwert für Rate (Rate Limit)**, um Grenzwerte für die Anweisungen für ein- und ausgehende Datenverkehrsrichtungen festzulegen.

b **Netzwerkdienst (Network Service)**: Wählen Sie eine der Optionen (**Direkt (Direct)**, **Mehrfachpfad (Multi-Path)** oder **Internet-Backhaul (Internet Backhaul)**) aus. Mit der Option **Direkt (Direct)** wird der Datenverkehr direkt an das Ziel gesendet, um das SD-WAN Gateway zu umgehen. Die Option „Internet-Backhaul (Internet Backhaul)“ kann nur für Internetregeln verwendet werden. Weitere Informationen zu diesen Optionen finden Sie im Abschnitt Konfigurieren des Aktionsnetzwerkdiensts.

c **Link-Steuerung (Link Steering)**: Wählen Sie eine der folgenden Optionen in der nachfolgenden Tabelle aus. (Informationen zu DSCP, zur DSCP-Markierung für Underlay- und Overlay-Datenverkehr finden Sie unter „Link-Steuerung: DSCP-Markierung für Underlay- und Overlay-Datenverkehr“.)

Option	Beschreibung
Automatisch (Auto)	Standardmäßig werden alle Anwendungen in den Modus für die automatische Link-Steuerung versetzt. Wenn sich eine Anwendung im Modus für die automatische Link-Steuerung befindet, wählt die DMPO-Funktion automatisch die besten Links basierend auf dem Anwendungstyp aus und aktiviert automatisch die bedarfsorientierte Standardisierung, falls erforderlich. Weitere Informationen zu diesem Thema finden Sie unter Link-Auswahl: Automatisch (Auto). Geben Sie im Dropdown-Menü ein DSCP-Tag für innere Pakete und ein DSCP-Tag für äußere Pakete ein.
Transportgruppe (Transport Group)	Eine Transportgruppe ist ein Paket von WAN-Links, die mit ähnlichen Merkmalen und Funktionen gruppiert sind. Eine Beschreibung der unten stehenden Transportgruppenoptionen finden Sie unter Link-Steuerung nach Transportgruppe. Wählen Sie im Dropdown-Menü**Öffentlich verkabelt (Public Wired)**, **Öffentlich drahtlos (Public Wireless)** oder **Privat verkabelt (Private Wired)** aus. Wählen Sie eine der folgenden Optionsschaltflächen aus: **Obligatorisch (Mandatory)**, **Bevorzugt (Preferred)** oder **Verfügbar (Available)**. Wählen Sie das DSP-Tag für innere Pakete und das DSP-Tag für äußere Pakete in den jeweiligen Dropdown-Menüs aus.

Option	Beschreibung
Schnittstelle (Interface)	Wählen Sie die folgenden Optionen für die Schnittstelle unten aus. Weitere Informationen finden Sie im Abschnitt mit dem Titel Link-Steuerung nach Schnittstelle. ■ Wählen Sie eine Schnittstelle aus dem Dropdown-Menü aus. ■ Geben Sie das VLAN in das Textfeld ein. **Hinweis** Das VLAN kann nicht angegeben werden, wenn der Netzwerkdienst mit Mehrfachpfad verwendet wird. ■ Wählen Sie eine der folgenden Optionsschaltflächen: „Obligatorisch (Mandatory)“, „Bevorzugt (Preferred)“, „Verfügbar (Available)“. Wenn Sie die Option „Bevorzugt (Preferred)“ wählen, wird das Kontrollkästchen **Fehlerkorrektur vor der Steuerung (Error Correct Before Steering)** angezeigt. Wenn Sie dieses Kontrollkästchen deaktivieren, steuert die Anwendung, bevor eine Fehlerkorrektur eintritt. ■ **ICMP-Test (ICMP Probe)**: Wählen Sie ggf. einen ICMP-Test aus dem Dropdown-Menü aus. ■ Wählen Sie das DSCP-Tag für innere Pakete und das DSCP-Tag für äußere Pakete in den jeweiligen Dropdown-Menüs aus.
WAN-Link (WAN Link)	Für diese Option ist die Schnittstellenkonfiguration getrennt und unterscheidet sich von der WAN-Link-Konfiguration. Sie können einen WAN-Link auswählen, der entweder manuell konfiguriert oder automatisch erkannt wurde. Wählen Sie aus dem Dropdown-Menü einen WAN-Link aus. Weitere Informationen finden Sie unter Dropdown-Menü „WAN-Link (WAN Link)“.

d **NAT**: Deaktivieren oder aktivieren Sie NAT. Weitere Informationen finden Sie im Abschnitt mit dem Titel Konfigurieren von richtlinienbasierter NAT.

e **Dienstklasse (Service Class)**: Wählen Sie eine Dienstklassenoption aus. Der Dienstklassenparameter kann auf „Echtzeit (Real-time)“ (zeitsensitiver Datenverkehr), „Transaktional (Transactional)“ oder „Massen (Bulk)“ festgelegt werden. Diese Option ist nur für eine benutzerdefinierte Anwendung vorgesehen. VMware SD-WAN-Anwendungen bzw. -Kategorien fallen in eine dieser Kategorien.

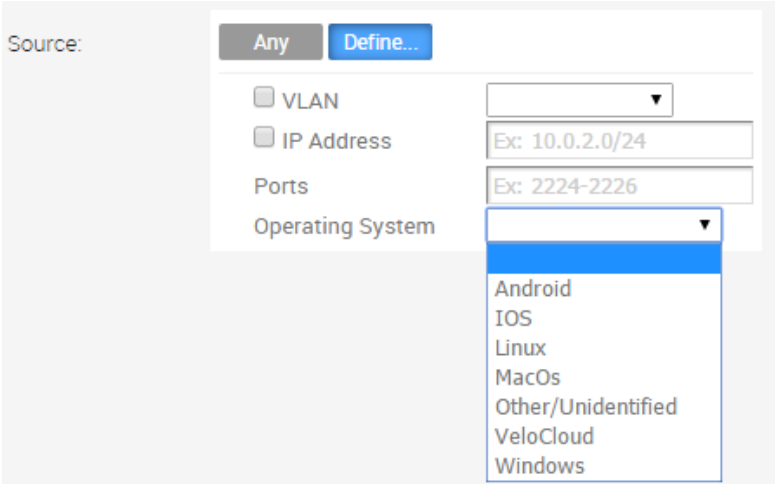
8 Klicken Sie auf **OK**, um Ihre Regel zu konfigurieren. Die Regel für die Unternehmensrichtlinie wird erfolgreich erstellt.

Referenz: Overlay-QoS-CoS-Zuordnung

Konfigurieren der Übereinstimmungsquelle

In diesem Abschnitt werden die Optionen **Übereinstimmungsquelle (Match Source)**, **Ziel (Destination)** und **Anwendung (Application)** im Detail erläutert. Für jede Übereinstimmungsauswahl wird die Option **Alle (Any)** verwendet, um Datenverkehr von einer Quelle, einem Ziel oder einer Anwendung zu bestimmen.

Bei Auswahl der Option **Definieren (Define)** für die Übereinstimmungsquelle kann der Quelldatenverkehr auf ein bestimmtes VLAN, eine IP-Adresse, einen Port, ein Betriebssystem oder eine beliebige Kombination von Auswahlmöglichkeiten eingegrenzt werden.



Konfigurieren des Übereinstimmungsziels

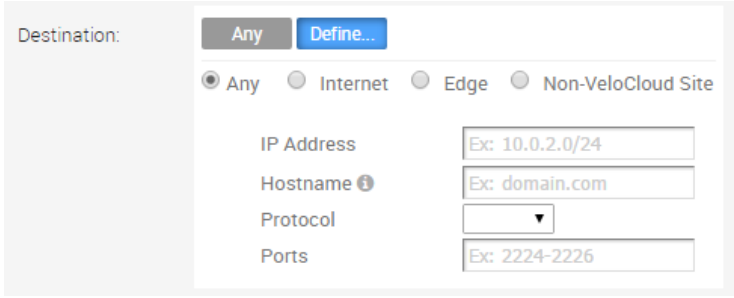
Geben Sie bei Auswahl der Option **Definition des Übereinstimmungsziels (Match Destination Define)** zusätzliche Parameter an, um das Datenverkehrsziel zu identifizieren.

Das Ziel kann zunächst auf einen Typ (**Alle (Any)**, **Internet**, **Edge** oder Non VMware SD-WAN Site) eingegrenzt werden. Eine Beschreibung der oben genannten Datenverkehrsziele finden Sie in der folgenden Tabelle.

Option	Beschreibung
Alle (Any)	Der gesamte Datenverkehr, unabhängig vom Ziel oder Routing.
Internet	Der Datenverkehr, der dazu bestimmt ist, ins Internet und nicht in das Netzwerk gesendet zu werden.
Edge	Der Datenverkehr, der für eine andere Site im Netzwerk bestimmt ist. Sites wie diese würden einen SD-WAN Edge verwenden.
Nicht-VeloCloud-Site (Non-VeloCloud Site)	Sites, die keinen SD-WAN Edge verwenden, aber eine Route innerhalb des Netzwerks haben. Eine Non VMware SD-WAN Site wird unter **Konfigurieren (Configure)** > **Netzwerkdienste (Network Services)** konfiguriert.

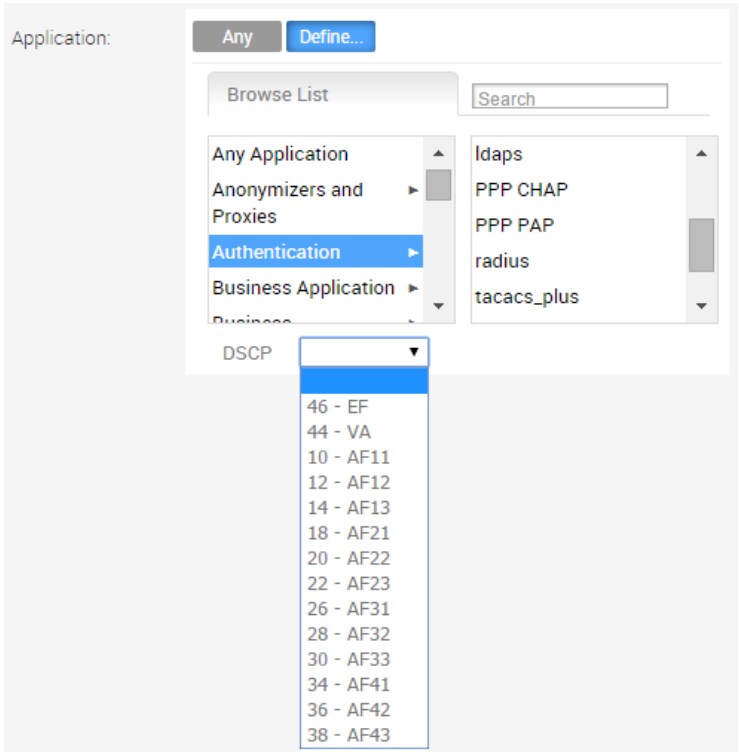
Das Ziel kann dann weiter definiert werden, indem eine **IP-Adresse (IP Address)**, ein **Hostname**, ein **Protokoll (Protocol)** (GRE, ICMP, TCP oder UDP) und ein Port angegeben werden.

Übereinstimmungsziel (Match Destination)-Optionen sind besonders nützlich, wenn dem gleichen Muster für die Datenverkehrsübereinstimmung je nach gewählter Route unterschiedliche QoS-Werte zugewiesen werden müssen. Als Beispiel können Sie dem Verkehr, der für eine VMware SD-WAN Site bestimmt ist, eine höhere Priorität zuweisen als dem regulären Internetverkehr aus der Cloud. Dies kann mit dem Wert für die Zielkonfiguration problemlos erreicht werden.



Konfigurieren der Übereinstimmungsanwendung

Wenn die Option **Definition der Anwendungsübereinstimmung (Match Application Define)** ausgewählt ist, können Anwendungen zuerst nach Kategorie und dann nach spezifischer Anwendung ausgewählt werden. Darüber hinaus kann ein DSCP-Wert so festgelegt werden, dass er den mit einem voreingestellten DSCP/TOS-Tag eingehenden Verkehr abgleicht.

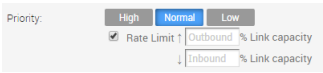


In den folgenden Abschnitten werden die Optionen **Aktion (Action) Priorität (Priority)**, **Netzwerkdienst (Network Service)**, **Link-Steuerung (Link Steering)**, NAT und **Dienstklasse (Service class)** im Detail erläutert.

Hinweis Abhängig von Ihren Auswahlmöglichkeiten für **Übereinstimmung (Match)** sind einige Aktionen möglicherweise nicht verfügbar. Wenn z. B. **Alle Anwendungen (All Applications)** ausgewählt ist, sind die Optionen **Netzwerkdienst (Network Service)** und **Link-Aktionen (Link Actions)** ausgegraut und stehen nicht zur Auswahl zur Verfügung. Wenn ein **Ziel (Destination)** des Typs **Internet** oder eine **Anwendung (Application)** des Typs **Routingfähige Apps (Routable Apps)** für ein VPN-Profil ausgewählt wurde, steht auf ähnliche Weise eine zusätzliche **Netzwerkdienst (Network Service)**-Option namens **Internet-Backhaul (Internet Backhaul)** zur Verfügung.

Konfigurieren der Aktionspriorität

Mit dem Aktionsparameter **Priorität (Priority)** kann der Datenverkehr als **Hoch (High)**, **Normal** oder **Niedrig (Low)** kategorisiert werden. Ein Prozentwert für **Grenzwert für Rate (Rate Limit)** kann für beide Richtungen angewendet werden: **Ausgehend (Outbound)** und **Eingehend (Inbound)**.



Konfigurieren des Aktionsnetzwerkdiensts

Beim Erstellen oder Aktualisieren einer Unternehmensrichtlinienregel und -aktion können Sie den **Netzwerkdienst (Network Service)** auf **Direkt (Direct)**, **Mehrfachpfad (Multi-Path)** und **Internet-Backhaul (Internet Backhaul)** festlegen.

Direkt (Direct)

Sendet den Verkehr aus der WAN-Leitung zum Ziel und umgeht dabei das SD-WAN Gateway. NAT wird auf den Datenverkehr angewendet, wenn das Kontrollkästchen **Direkter NAT-Datenverkehr (NAT Direct Traffic)** in den **Schnittstelleneinstellungen (Interface Settings)** auf der Registerkarte **Gerät (Device)** aktiviert ist. Berücksichtigen Sie bei der Konfiguration von direktem NAT-Datenverkehr die folgenden Einschränkungen.

- NAT muss den Datenverkehr in der Edge-Routing-Tabelle mit dem nächsten Hop entweder als Cloud-VPN oder Cloud-Gateway treffen.
- NAT funktioniert nur für den Datenverkehr zu öffentlichen IP-Adressen, auch wenn die Unternehmensrichtlinie die Konfiguration privater IP-Adressen als Ziel erlaubt.

Mehrfachpfad (Multi-Path)

Sendet den Datenverkehr von einem SD-WAN Edge an einen anderen SD-WAN Edge.

Internet-Backhaul (Internet Backhaul)

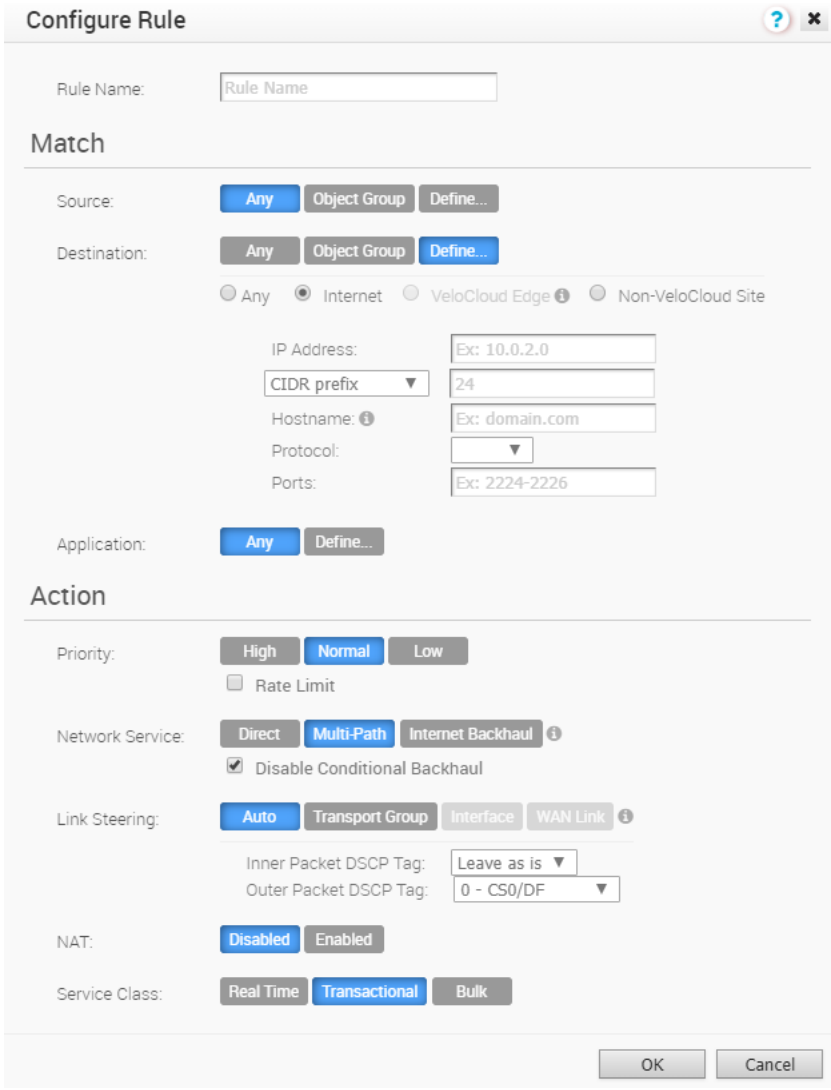
Wenn Sie bei der Konfiguration der Übereinstimmungskriterien für die Unternehmensrichtlinienregel das **Ziel (Destination)** als **Internet** festlegen, wird der **Internet-Backhaul (Internet Backhaul)**-Netzwerkdienst aktiviert.

Hinweis Der **Internet-Backhaul (Internet Backhaul)**-Netzwerkdienst gilt nur für Internetdatenverkehr (WAN-Datenverkehr, der für Netzwerkpräfixe bestimmt ist, die nicht mit einer bekannten lokalen Route oder VPN-Verbindung übereinstimmen).

Wenn **Internet-Backhaul (Internet Backhaul)** ausgewählt ist, müssen Sie eine der folgenden Optionen auswählen:

- **Backhaul-Hubs (Backhaul Hubs)**
- **Nicht-VeloCloud-Site (Non-VeloCloud Site)**
- **Cloud-Sicherheitsdienst (Cloud Security Service)**

Sie sollten in der Lage sein, mehrere VMware SD-WAN Sites-Instanzen für Backhaul zu konfigurieren, um die Redundanz zu unterstützen, die inhärent in die Non VMware SD-WAN Site-Verbindung eingebaut ist, aber ein konsistentes Verhalten der Nichtverfügbarkeit des Diensts beibehalten, das zu einem Ausfall des Datenverkehrs führt.



Wenn bedingter Backhaul auf der Profilebene aktiviert ist, gilt er standardmäßig für alle für dieses Profil konfigurierten Unternehmensrichtlinien. Sie können den bedingten Backhaul für ausgewählte Richtlinien deaktivieren, um dieses Verhalten für den ausgewählten Datenverkehr („Direkt“ und „Mehrfachpfad“) auszuschließen. Aktivieren Sie dazu das Kontrollkästchen **Bedingten Backhaul deaktivieren (Disable Conditional Backhaul)** im Bereich **Aktion (Action)** im Bildschirm **Regel konfigurieren (Configure Rule)** für die ausgewählte Unternehmensrichtlinie. Weitere Informationen finden Sie unter Bedingter Backhaul.

Konfigurieren der Aktionslink-Steuerung

In der Unternehmensrichtlinie gibt es vier Modi für die Link-Steuerung: **Automatisch (Auto)**, **Transportgruppe (Transport Group)**, **WAN-Link (WAN Link)** und **Schnittstellen (Interfaces)**.

Hinweis Weitere Informationen zu öffentlichen bzw. privaten WAN-Links, Schnittstellenkonfiguration und benutzerdefinierten Optionen finden Sie in den entsprechenden Abschnitten, die unter den folgenden Links verfügbar sind.

Link-Auswahl: Automatisch (Auto)

Standardmäßig erhalten alle Anwendungen den Modus für die automatische Link-Steuerung. Das bedeutet, dass DMPO automatisch die besten Links basierend auf dem Anwendungstyp auswählt und bei Bedarf automatisch die bedarfsorientierte Standardisierung aktiviert. Es gibt vier mögliche Kombinationen der Link-Steuerung und bedarfsorientierten Standardisierung für Internetanwendungen. Wie bereits erwähnt, durchläuft der Datenverkehr innerhalb des Unternehmens (VPN) immer die DMPO-Tunnel. Daher können die Vorteile der bedarfsorientierten Standardisierung immer genutzt werden.

Szenario	Erwartetes DMPO-Verhalten
Mindestens ein Link erfüllt die SLA für die Anwendung.	Wählen Sie den besten verfügbaren Link aus.
Ein einziger Link mit einem Paketverlust, der die SLA für die Anwendung überschreitet.	Aktivieren Sie FEC für die Echtzeitanwendungen, die auf diesem Link gesendet werden.
Zwei Links mit Verlust auf nur einem Link.	Aktivieren Sie FEC auf beiden Links.
Mehrere Links mit Verlust auf mehreren Links.	Aktivieren Sie FEC auf den beiden besten Links.
Zwei Links, aber ein Link wird als instabil angezeigt, d. h., es fehlen drei aufeinanderfolgende Taktsignale.	Markieren Sie den Link als unbrauchbar und lenken Sie den Datenfluss auf den nächsten besten verfügbaren Link.
Sowohl Jitter als auch Verlust auf beiden Links.	Aktivieren Sie FEC auf beiden Links und aktivieren Sie den Jitter-Puffer auf der Empfangsseite. Jitter-Puffer ist aktiviert, wenn Jitter größer als 7 ms für Audio und größer als 5 ms für Video ist. Der sendende DMPO-Endpoint benachrichtigt den empfangenden DMPO-Endpoint, um Jitter-Puffer zu aktivieren. Der empfangende DMPO-Endpoint puffert bis zu 10 Pakete oder 200 ms an Datenverkehr, je nachdem, was zuerst eintritt. Der empfangende DMPO-Endpoint verwendet den ursprünglichen Zeitstempel, der in der DMPO-Kopfzeile eingebettet ist, um die Flow-Rate zu berechnen, die im Puffer zur Jitter-Aufhebung verwendet werden soll. Wenn der Datenfluss nicht mit einer konstanten Geschwindigkeit gesendet wird, wird der Jitter-Puffer deaktiviert.

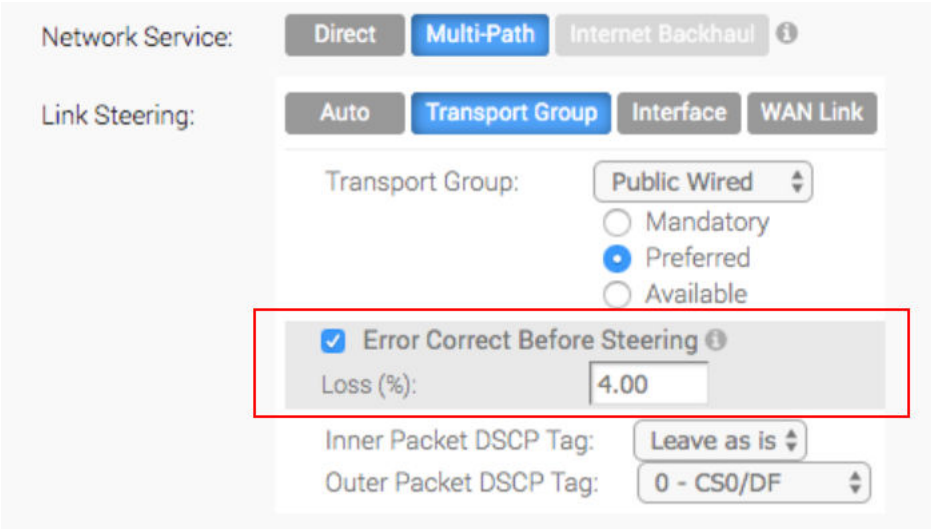
Link-Steuerung nach Transportgruppe

Eine Transportgruppe stellt WAN-Links dar, die auf der Grundlage ähnlicher Merkmale und Funktionen gebündelt sind. Das Definieren einer Transportgruppe ermöglicht geschäftliche Abstraktion, sodass eine ähnliche Richtlinie auf verschiedene Hardwaretypen angewendet werden kann.

Verschiedene Standorte können über unterschiedliche WAN-Transporte verfügen (z. B. WAN-Betreibername, WAN-Schnittstellenname). DMPO verwendet das Konzept der Transportgruppe, um die zugrunde liegenden WAN-Betreiber und -Schnittstellen von der Unternehmensrichtlinienkonfiguration zu abstrahieren. Die Unternehmensrichtlinienkonfiguration kann die Transportgruppe (öffentliches verkabelt, öffentliches drahtlos, private verkabelt usw.) in der Steuerungsrichtlinie angegeben, sodass dieselbe Konfiguration der Unternehmensrichtlinie auf verschiedene Gerätetypen oder Standorte angewendet werden kann, die völlig unterschiedliche WAN-Betreiber und WAN-Schnittstellen haben können. Wenn die DMPO die WAN-Link-Erkennung durchführt, weist sie auch die Transportgruppe dem WAN-Link zu. Dies ist die wünschenswerteste Option für die Angabe der Links in der Unternehmensrichtlinie, da IT-Administratoren dadurch nicht mehr die Art der physischen Verbindung oder den WAN-Betreiber kennen müssen.

Wenn Sie die Option **Bevorzugt (Preferred)** wählen, wird das Kontrollkästchen **Fehlerkorrektur vor der Steuerung (Error Correct Before Steering)** angezeigt.

Wenn Sie das Kontrollkästchen **Fehlerkorrektur vor der Steuerung (Error Correct Before Steering)** aktivieren, wird das variable Textfeld „Verlust % (Loss%)“ angezeigt. Wenn Sie einen Prozentsatz für den Verlust festlegen (z. B. 4 %), verwendet der Edge weiterhin den ausgewählten Link oder die ausgewählte Transportgruppe und wendet die Fehlerkorrektur an, bis der Verlust 4 % erreicht, wenn der Datenverkehr in einen anderen Pfad gelenkt wird. (Siehe Abbildung unten.) Wenn das Kontrollkästchen **Fehlerkorrektur vor der Steuerung (Error Correct Before Steering)** deaktiviert ist, beginnt der Edge mit der Steuerung des Datenverkehrs, wenn der Verlust für den Link die Anwendungs-SLA überschreitet, d. h., die Echtzeit-Anwendungs-SLA beträgt standardmäßig 0,3 %. Wenn Sie dieses Kontrollkästchen deaktivieren, beginnt die Anwendung mit der Steuerung, bevor eine Fehlerkorrektur eintritt.



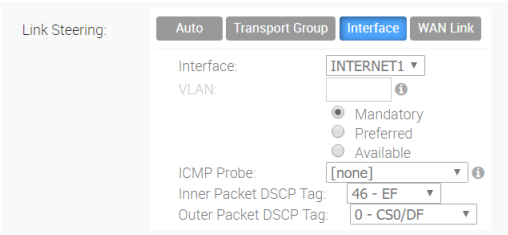
Hinweis Diese Option ist sowohl auf der Ebene „Edge-Außerkraftsetzung (Edge Override)“ als auch auf der Profilebene zulässig.

Link-Steuerung nach Schnittstelle

Für diese Option ist die Link-Steuerung an eine physische Schnittstelle gebunden. Die Link-Steuerung nach Schnittstelle wird primär für das Routing verwendet. Auch wenn sie logischerweise nur für das Routing des Datenverkehrs direkt von der VMware SD-WAN Site aus verwendet werden sollte, wählt sie, wenn die angegebene Regel über einen Netzwerkdienst mit angeforderter Internet-Mehrfachpfad-Funktion verfügt, einen einzigen WAN-Link aus, der mit der Schnittstelle verbunden ist.

Wenn Sie die Option **Bevorzugt (Preferred)** wählen, wird das Kontrollkästchen **Fehlerkorrektur vor der Steuerung (Error Correct Before Steering)** angezeigt. Wenn Sie prüfen, ob das Kontrollkästchen aktiviert ist, wird eine zusätzliche Variable für den Verlustprozentsatz verfügbar. Wenn die Option deaktiviert ist, beginnt der Edge, den Datenverkehr abzuleiten, wenn der Verlust für den Link die Anwendungs-SLA überschreitet, d. h., die Echtzeit-Anwendungs-SLA beträgt standardmäßig 0,3 %. Wenn „Fehlerkorrektur vor der Steuerung (Error Correct Before Steering)“ angewendet und der Verlustprozentsatz definiert wird, in diesem Beispiel 4 %, verwendet der Edge weiterhin den ausgewählten Link oder die Transportgruppe und wendet die Fehlerkorrektur an, bis der Verlust 4 % erreicht. Wird dieser Wert überschritten, wird der Datenverkehr auf einen anderen Pfad geleitet. Wenn Sie dieses Kontrollkästchen deaktivieren, beginnt die Anwendung mit der Steuerung, bevor eine Fehlerkorrektur eintritt.

Hinweis Diese Option ist nur auf der Ebene „Edge-Außerkraftsetzung (Edge Override)“ zulässig. Dadurch wird sichergestellt, dass die bereitgestellten Link-Optionen immer mit dem SD-WAN Edge-Hardwaremodell übereinstimmen.



WAN-Link (WAN Link)

Für diese Option ist die Schnittstellenkonfiguration getrennt und unterscheidet sich von der WAN-Link-Konfiguration. Sie können einen WAN-Link auswählen, der entweder manuell konfiguriert oder automatisch erkannt wurde.

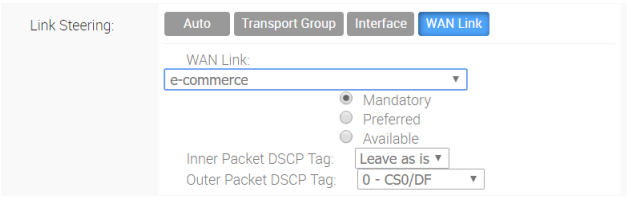
Dropdown-Menü „WAN-Link (WAN Link)“

Sie können Richtlinienregeln basierend auf bestimmten privaten Links definieren. Wenn Sie private Netzwerknamen erstellt und sie einzelnen privaten WAN-Overlays zugewiesen haben, werden diese Namen der privaten Links im Dropdown-Menü **WAN-Link (WAN Link)** angezeigt.

Informationen zum Definieren mehrerer Namen für private Netzwerke und zum Zuweisen dieser Netzwerke zu einzelnen privaten WAN-Overlays finden Sie unter Private Netzwerknamen und *Auswählen des Namens eines privaten Links*.

Wenn Sie die Option **Bevorzugt (Preferred)** wählen, wird das Kontrollkästchen **Fehlerkorrektur vor der Steuerung (Error Correct Before Steering)** angezeigt. Wenn Sie dieses Kontrollkästchen deaktivieren, beginnt die Anwendung mit der Steuerung, bevor eine Fehlerkorrektur eintritt.

Hinweis Diese Option ist nur auf der Ebene „Edge-Außerkraftsetzung (Edge Override)“ zulässig.

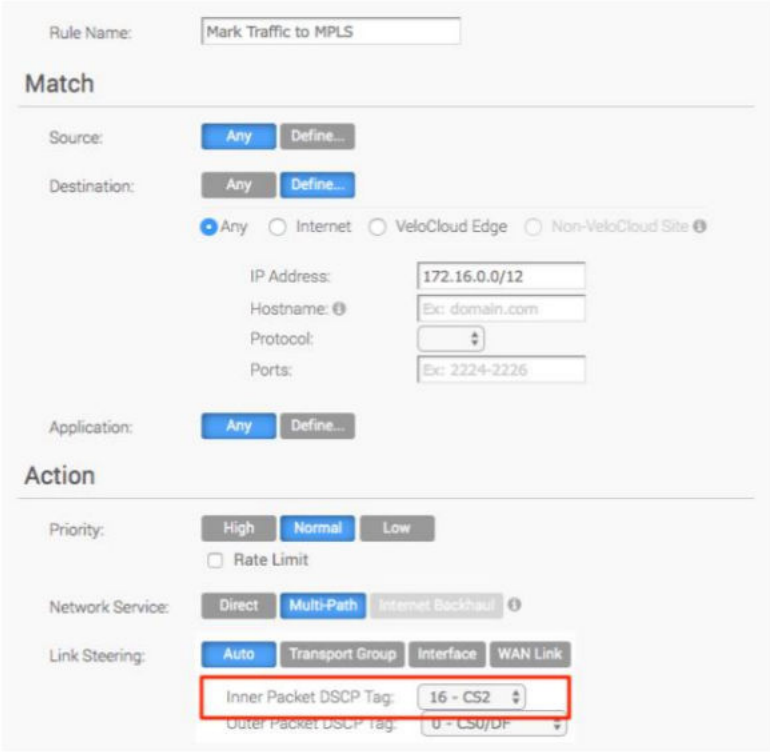


Zwecks Auswahl **nach Schnittstelle (by Interface)** und **nach WAN-Link (by WAN Link)** müssen Sie eine der folgenden Optionen auswählen:

Option	Beschreibung
Obligatorisch (Mandatory)	Zeigt an, dass der Datenverkehr über den WAN-Link oder die angegebene Link-Dienstgruppe gesendet werden soll. Wenn der angegebene Link (oder alle Links innerhalb der ausgewählten Dienstgruppe) inaktiv ist **oder** wenn ein Mehrfachpfad-Gateway nicht verfügbar ist, wird das entsprechende Paket verworfen.
Bevorzugt (Preferred)	Zeigt an, dass der Datenverkehr vorzugsweise über den WAN-Link oder die angegebene Link-Dienstgruppe gesendet werden soll. Wenn der angegebene Link (oder alle Links innerhalb der ausgewählten Dienstgruppe) inaktiv ist, wenn die ausgewählte Route für das Mehrfachpfad-Gateway instabil ist oder wenn das Link-SLO (Service Level Objective) nicht erfüllt wird, wird das entsprechende Paket auf den nächstbesten verfügbaren Link gelenkt. Wenn der bevorzugte Link wieder verfügbar wird, wird der Datenverkehr zurück an den bevorzugten Link geleitet.
Verfügbar (Available)	Zeigt an, dass der Datenverkehr vorzugsweise über den WAN-Link oder die angegebene Link-Dienstgruppe gesendet werden soll, sofern er verfügbar ist (unabhängig vom Link-SLO). Wenn der angegebene Link (oder alle Links innerhalb der ausgewählten Dienstgruppe) nicht verfügbar ist oder wenn die ausgewählte Route für das Mehrfachpfad-Gateway nicht verfügbar ist, wird das entsprechende Paket auf den nächsten verfügbaren Link gelenkt. Wenn der bevorzugte Link wieder verfügbar wird, wird der Datenverkehr zurück zum verfügbaren Link gelenkt.

Link-Steuerung: DSCP-Markierung für Underlay- und Overlay-Datenverkehr — Übersicht

VMware SD-WAN unterstützt die erneute DSCP-Markierung von Paketen, die vom Edge an den Underlay weitergeleitet werden. Der VMware SD-WAN Edge kann den auf einem WAN-Link weitergeleiteten Datenverkehr neu markieren, solange „Underlay-Berechnung (Underlay Accounting)“ auf der Schnittstelle aktiviert ist. Das erneute Markieren von DSCP ist in der Konfiguration der Unternehmensrichtlinie im Bereich „Link-Steuerung (Link Steering)“ aktiviert. Weitere Informationen finden Sie unter Erstellen einer Unternehmensrichtlinie. In dem unten gezeigten Beispielbild (unter der Annahme, dass der Edge mit MPLS verbunden ist, wobei sowohl Underlay- als auch Overlay-Datenverkehr an MPLS weitergeleitet wird) markiert der Edge, wenn der Datenverkehr mit dem Netzwerk-Präfix 172.16.0.0/12 übereinstimmt, die Underlay-Pakete erneut mit einem DSCP-Wert von 16 oder CS2 und ignoriert das Feld „DSCP-Tag für äußere Pakete (Outer Packet DSCP Tag)“. Für den an MPLS gesendeten Overlay-Datenverkehr, der derselben Unternehmensrichtlinie entspricht, wird der Wert für den DSCP für den äußeren Header auf das „DSCP-Tag für äußere Pakete (Outer Packet DSCP Tag)“ festgelegt.

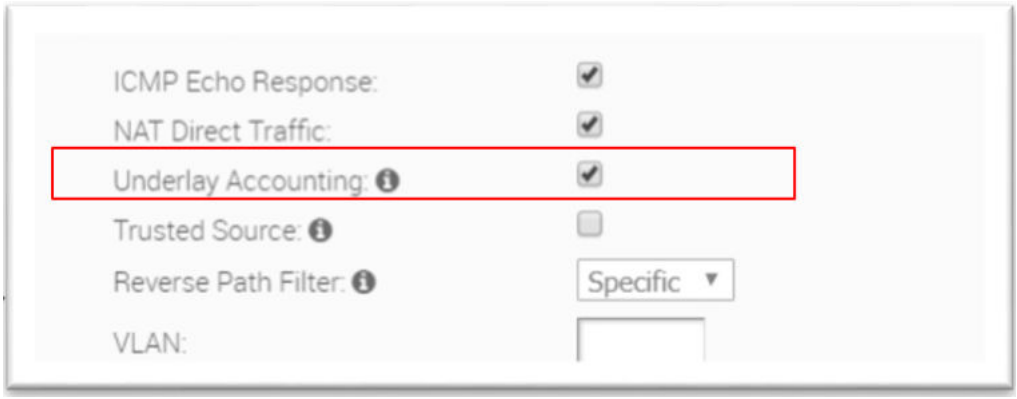


Link-Steuerung: DSCP-Markierung für Underlay- und Overlay-Datenverkehr — Anwendungsbeispiel

Edges, die mit MPLS verbunden sind, markieren normalerweise DSCP auf dem Paket, bevor sie an die PE gesendet werden, damit der Dienstanbieter das Paket in Übereinstimmung mit der SLA behandeln kann. „Underlay-Berechnung (Underlay Accounting)“ muss auf der WAN-Schnittstelle aktiviert sein, damit DSCP auf dem Underlay-Datenverkehr über die Unternehmensrichtlinie wirksam wird.

Link-Steuerung: Underlay-DSCP-Konfiguration

1 Stellen Sie sicher, dass „Underlay-Berechnung (Underlay Accounting)“ für WAN-Overlay standardmäßig in der SD-WAN Orchestrator-Instanz konfiguriert ist (Bereich **Konfigurieren (Configure)** > **Edge-Geräte (Edge Devices)** >**Geräteeinstellungen (Device Settings)**). Siehe Abbildung unten.



2 Navigieren Sie in SD-WAN Orchestrator zu **Konfigurieren (Configure)** > **Edges**>**Unternehmensrichtlinie (Business Policy)**.

3 Klicken Sie im Bildschirm **Unternehmensrichtlinie (Business Policy)** auf eine vorhandene Regel oder klicken Sie auf die Schaltfläche **Neue Regel (New Rule)**, um eine neue Regel zu erstellen.

4 Navigieren Sie im Abschnitt **Aktion (Action)** zum Bereich **Link-Steuerung (Link Steering)**.

5 Klicken Sie auf eine der folgenden Optionen, falls zutreffend: „Automatisch (Auto)“, „Transportgruppe (Transport Group)“, „Schnittstelle (Interface)“ oder „WAN-Link (WAN Link)“.

6 Konfigurieren Sie die **Übereinstimmung**skriterien für den Underlay-Datenverkehr und die Konfiguration für das DSCP-Tag für innere Pakete. Siehe Abbildung unten.

Link-Steuerung: Overlay-DSCP-Konfiguration

1 Stellen Sie sicher, dass „Underlay-Berechnung (Underlay Accounting)“ für WAN-Overlay standardmäßig in der SD-WAN Orchestrator-Instanz konfiguriert ist (Bereich **Konfigurieren (Configure)** > **Edge-Geräte (Edge Devices)** > **Geräteeinstellungen (Device Settings)**). Siehe Abbildung oben.

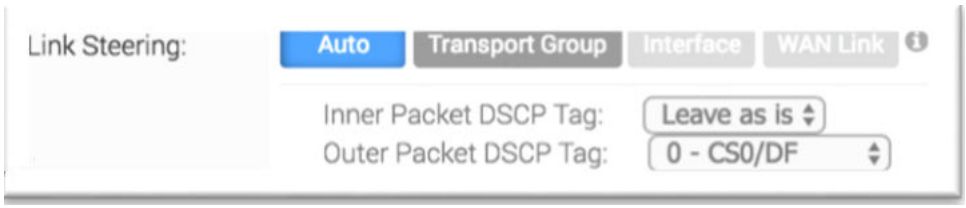
2 Navigieren Sie in SD-WAN Orchestrator zu **Konfigurieren (Configure)** > **Edges** > **Unternehmensrichtlinie (Business Policy)**.

3 Klicken Sie im Bildschirm **Unternehmensrichtlinie (Business Policy)** auf eine vorhandene Regel oder klicken Sie auf die Schaltfläche **Neue Regel (New Rule)**, um eine neue Regel zu erstellen.

4 Navigieren Sie im Abschnitt **Aktion (Action)** zum Bereich **Link-Steuerung (Link Steering)**.

5 Klicken Sie auf eine der folgenden Optionen, falls zutreffend: „Automatisch (Auto)“, „Transportgruppe (Transport Group)“, „Schnittstelle (Interface)“ oder „WAN-Link (WAN Link)“.

6 Konfigurieren Sie die **Übereinstimmung**skriterien für den Overlay-Datenverkehr und die Konfiguration für das DSCP-Tag für innere und äußere Pakete. Siehe Abbildung unten.



Konfigurieren von richtlinienbasierter NAT

Sie können die richtlinienbasierte NAT sowohl für die Quelle als auch für das Ziel konfigurieren. Die NAT kann mithilfe von Multipath entweder auf Non VMware SD-WAN Site-Datenverkehr oder auf den Internetdatenverkehr angewendet werden. Wenn Sie NAT konfigurieren, müssen Sie festlegen, welcher Datenverkehr mit NAT konfiguriert und welche Aktion durchgeführt werden soll. Es gibt zwei Typen von NAT-Konfigurationen: „Viele-zu-eins“ und „Eins-zu-eins“.

Zugriff auf NAT

Sie können auf die NAT-Funktion über **Konfigurieren > Profile > Registerkarte „Unternehmensrichtlinie“ (Configure > Profiles > Business Policy tab)** zugreifen und anschließend auf die Schaltfläche **Neue Regel (New Rule)** klicken. Die NAT-Funktion befindet sich im Bereich **Aktion (Action)**.

NAT-Konfiguration vom Typ „Viele-zu-eins“

In dieser Konfiguration können Sie die Quell- oder Ziel-IP des Datenverkehrs, die von den Hosts hinter dem Edge stammt, per NAT an eine andere eindeutige Quell- oder Ziel-IP-Adresse senden. Beispielsweise kann der Benutzer für alle Datenflüsse, die für einen Host oder Server im Datencenter, das sich hinter dem Partner-Gateway mit einer eindeutigen IP-Adresse befindet, eine Quell-NAT durchführen, auch wenn sie von verschiedenen Hosts hinter einem Edge stammen.

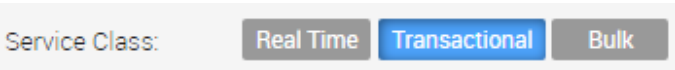
Die folgende Abbildung zeigt ein Beispiel der „Viele-zu-eins“-Konfiguration. In diesem Beispiel erhält der gesamte Datenverkehr, der von den Hosts stammt, die mit VLAN **100 - Unternehmen 2 (100 - Corporate 2)** verbunden sind (hinter dem Edge, der für einen Internet-Host oder einen Host hinter dem DC bestimmt ist), Quell-NAT mit der IP-Adresse 72.4.3.1.

NAT-Konfiguration vom Typ „Eins-zu-eins“

In dieser Konfiguration leitet der Zweigstellen-Edge eine einzelne lokale IP-Adresse eines Hosts oder Servers an eine andere globale IP-Adresse per NAT weiter. Wenn der Host in der Non VMware SD-WAN Site oder im Datencenter Datenverkehr an die globale IP-Adresse sendet (konfiguriert als Quell-NAT-IP-Adresse in der NAT-Konfiguration vom Typ „Eins-zu-eins“), leitet das SD-WAN Gateway diesen Datenverkehr an die lokale IP-Adresse des Hosts oder Servers in der Zweigstelle weiter.

Konfigurieren einer Aktionsdienstklasse

Der Dienstklassenparameter kann auf **Echtzeit (Real Time)** (zeitsensibler Datenverkehr), **Transaktional (Transactional)** oder **Massen (Bulk)** festgelegt werden. Diese Option ist nur für eine benutzerdefinierte Anwendung vorgesehen. VMware SD-WANAnwendungen/Kategorien gehören zu einer dieser Kategorien.



Overlay-QoS-CoS-Zuordnung

Eine Datenverkehrsklasse wird durch eine Kombination aus Priorität (Hoch (High), Normal oder Niedrig (Low)) und Dienstklasse (Echtzeit (Real-Time), Transaktional (Transactional) oder Massen (Bulk)) definiert, die zu einer 3x3-Matrix mit neun Datenverkehrsklassen führt. Sie können die Gewichtung von Anwendung/Kategorie und Planer diesen Datenverkehrsklassen zuordnen. Alle Anwendungen innerhalb einer Verkehrsklasse werden mit der aggregierten QoS-Behandlung angewendet, einschließlich Planung (Scheduling) und Überwachung (Policing).

Alle Anwendungen in einer bestimmten Datenverkehrsklasse verfügen über eine garantierte minimale aggregierte Bandbreite während der Überlastung basierend auf der Planergewichtung (oder dem Prozentsatz der Bandbreite). Wenn keine Überlastung vorhanden ist, sind die Anwendungen in der maximal aggregierten Bandbreite zulässig. Ein Policer kann angewendet werden, um die Bandbreite für alle Anwendungen in einer bestimmten Datenverkehrsklasse zu begrenzen. Die nachstehende Abbildung zeigt eine Standardkonfiguration der Anwendung/Kategorie und Datenverkehrsklassen-Zuordnung.

Die Unternehmensrichtlinie beinhaltet die einsatzbereite Funktion für intelligente Standardwerte, die mehr als 2.500 Anwendungen Datenverkehrsklassen zuordnet. Sie können anwendungsbezogene QoS verwenden, ohne eine Richtlinie definieren zu müssen. Jeder Datenverkehrsklasse wird im Planer eine Standardgewichtung zugewiesen, und diese Parameter können in der Unternehmensrichtlinie geändert werden. Nachfolgend finden Sie die Standardwerte für die 3x3-Matrix mit neun Datenverkehrsklassen. Die nachstehende Abbildung zeigt eine Standardkonfiguration der Gewichtungs- und Datenverkehrsklassen-Zuordnung.

Beispiel:

In diesem Beispiel hat ein Kunde eine Internetverbindung mit 90 Mbit/s und 10 Mbit/s MPLS auf dem Edge. Die Gesamtbandbreite beträgt 100 Mbit/s. Basierend auf der obigen Standardzuordnung für Gewichtung und Datenverkehrsklasse verfügen alle Anwendungen, die der geschäftlichen Zusammenarbeit zugeordnet sind, über eine garantierte Bandbreite von 35 MBit/s, und alle Anwendungen, die E-Mails zugeordnet sind, verfügen über eine garantierte Bandbreite von 15 Mbit/s. Beachten Sie, dass Unternehmensrichtlinien für eine ganze Kategorie wie geschäftliche Zusammenarbeit, Anwendungen (z. B. Skype for Business) sowie detailgenauere Unteranwendungen (z. B. Skype-Dateiübertragung, Skype Audio und Skype Video) definiert werden können.

Konfigurieren der Overlay-QoS-CoS-Zuordnung

Hinweis Die Funktion „SD-WAN-Datenverkehrsklassen- und Gewichtungszuordnung“ (SD-WAN Traffic Class and Weight Mapping) kann nur bearbeitet werden, wenn sie von Ihrem Operator aktiviert wird. Um Zugriff auf diese Funktion zu erhalten, wenden Sie sich an Ihren Operator.

So aktivieren Sie die Overlay-QoS-CoS-Zuordnung:

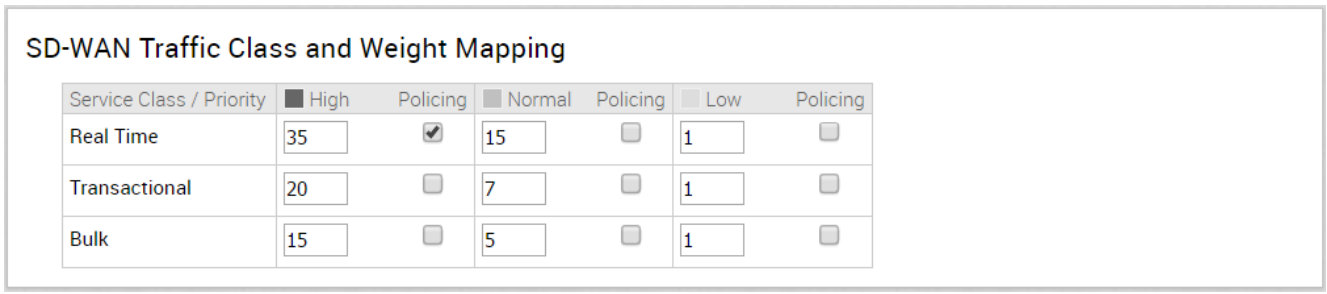
1 Navigieren Sie zu **Konfigurieren (Configure) > Profile (Profiles)**.

2 Klicken Sie auf den Link des entsprechenden Konfigurationsprofils.

3 Klicken Sie auf die Registerkarte **Unternehmensrichtlinie (Business Policy)**.

4 Geben Sie im Bereich **SD-WAN-Datenverkehrsklassen- und Gewichtungszuordnung (SD-WAN Traffic Class and Weight Mapping)** nach Bedarf die numerischen Werte für **Echtzeit (Real Time)**, **Transaktional (Transactional)** und/oder **Massen (Bulk)** ein.

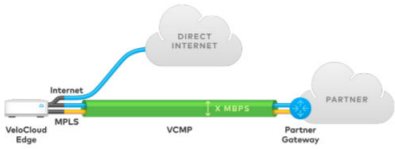
5 Aktivieren Sie bei Bedarf das Kontrollkästchen **Überwachung (Policing)** für eine Dienstklasse.



Tunnel Shaper für Dienstanbieter mit Partner-Gateway

In diesem Abschnitt wird der Tunnel Shaper für Dienstanbieter mit dem Partner-Gateway beschrieben.

Dienstanbieter können SD-WAN-Dienste mit einer geringeren Kapazität anbieten als die aggregierte Kapazität der WAN-Verbindungen in der lokalen Zweigstelle. Beispielsweise können Kunden eine Breitbandverbindung von einem anderen Anbieter und SP erworben haben, der SD-WAN-Dienste anbietet, und das Hosting-VMware SD-WAN-Partner-Gateway hat keine Kontrolle über die zugrunde liegende Breitbandverbindung. Um sicherzustellen, dass die Kapazität des SD-WAN-Diensts eingehalten wird, und um eine Überlastung in Richtung Partner-Gateway zu vermeiden, kann ein Dienstanbieter in solchen Situationen den DMPO Tunnel Shaper zwischen dem Tunnel und dem Partner-Gateway aktivieren.



Tunnel Shaper – Beispiel:

Wie im obigen Diagramm dargestellt, verfügt der SD-WAN Edge über zwei Verbindungen, 20 Mbit/s Internet und 20 Mbit/s MPLS, mit einem 35-Mbit/s-SD-WAN-Dienst des SP. Um sicherzustellen, dass der Datenverkehr zum Partner-Gateway 35 Mbit/s (in der obigen Abbildung als „X“ angezeigt) nicht überschreitet, kann ein Dienstanbieter einen Tunnel Shaper auf dem DMPO-Tunnel platzieren.

Konfigurieren der Ratenbegrenzung für Tunneldatenverkehr

Hinweis Die Funktion „Ratenbegrenzung für Tunneldatenverkehr“ (Rate-Limit Tunnel Traffic) kann nur bearbeitet werden, wenn sie vom Operator aktiviert wurde. Um Zugriff auf diese Funktion zu erhalten, wenden Sie sich an Ihren Operator.

So aktivieren Sie die Funktion „Ratenbegrenzung für Tunneldatenverkehr“ (Rate-Limit Tunnel Traffic):

1 Gehen Sie im Navigationsbereich zu **Konfigurieren (Configure) > Profile (Profiles)**.

2 Klicken Sie auf den Link des entsprechenden Konfigurationsprofils.

3 Klicken Sie auf die Registerkarte **Unternehmensrichtlinie (Business Policy)**.

4 Aktivieren Sie im Bereich **SD-WAN-Overlay-Ratenbegrenzung (SD-WAN Overlay Rate Limit)** das Kontrollkästchen **Ratenbegrenzung für Tunneldatenverkehr (Rate-Limit Tunnel Traffic)**. (Siehe Abbildung unten.)

5 Wählen Sie das Optionsfeld **Prozent (Percent)** oder **Rate (Mbit/s) (Rate (Mbps))** aus.

6 Geben Sie im Textfeld **Grenzwert (Limit)** einen numerischen Grenzwert für den Tunneldatenverkehr ein.

7 Klicken Sie auf **Änderungen speichern (Save Changes)**.

Konfigurieren der Firewall

12

Eine Firewall ist ein Netzwerksicherheitsgerät, das den eingehenden und ausgehenden Netzwerkdatenverkehr überwacht und festlegt, ob bestimmter Datenverkehr basierend auf einem definierten Satz von Sicherheitsregeln zugelassen oder blockiert werden soll. SD-WAN Orchestrator unterstützt die Konfiguration von statusfreien und statusbehafteten Firewalls für Profile und Edges.

Eine statusbehaftete Firewall überwacht und verfolgt den Betriebszustand und die Merkmale aller Netzwerkverbindungen, die über die Firewall kommen, und verwendet diese Informationen, um zu ermitteln, welche Netzwerkpakete die Firewall passieren sollen. Die statusbehafteten Firewalls erstellen eine Statustabelle und verwenden diese Tabelle, um nur den Datenverkehr von den aktuell in der Statustabelle aufgeführten Verbindungen zuzulassen. Nachdem eine Verbindung aus der Statustabelle entfernt wurde, ist kein Datenverkehr vom externen Gerät dieser Verbindung zulässig.

Die statusbehaftete Firewallfunktion bietet die folgenden Vorteile:

- Verhinderung von Angriffen wie Denial of Service (DoS) und Spoofing
- Stabilere Protokollierung
- Verbesserte Netzwerksicherheit

Hinweis Standardmäßig ist die Funktion **Statusbehaftete Firewall (Stateful Firewall)** für ein Unternehmen aktiviert. SD-WAN Orchestrator ermöglicht dem Unternehmensbenutzer die Aktivierung oder Deaktivierung der statusbehaftete Firewallfunktion auf Profil- und Edge-Ebene auf der Seite **Firewall**. Um die statusbehaftete Firewallfunktion für ein Unternehmen zu deaktivieren, wenden Sie sich an einen Operator mit der Superuser-Berechtigung.

Hinweis Asymmetrisches Routing wird für Edges mit aktivierter statusbehafteter Firewall nicht unterstützt.

Hinweis Standardmäßig ist die Funktion **Syslog-Weiterleitung (Syslog Forwarding)** für ein Unternehmen deaktiviert. Um Firewallprotokolle aus einem Unternehmens-SD-WAN Edges in einer oder mehreren zentralen Remote-Syslog-Collector-Instanzen zu sammeln, muss ein Unternehmensbenutzer diese Funktion auf Unternehmensebene aktivieren. Weitere Informationen zum Konfigurieren von Syslog Collector-Details pro Segment in der SD-WAN Orchestrator-Instanz finden Sie unter Konfigurieren von Syslog-Einstellungen auf der Profilebene.

Informationen zum Konfigurieren von Firewalleinstellungen auf Profil- und Edge-Ebene finden Sie unter:

- Konfigurieren der Firewall für Profile
- Konfigurieren der Firewall für Edges

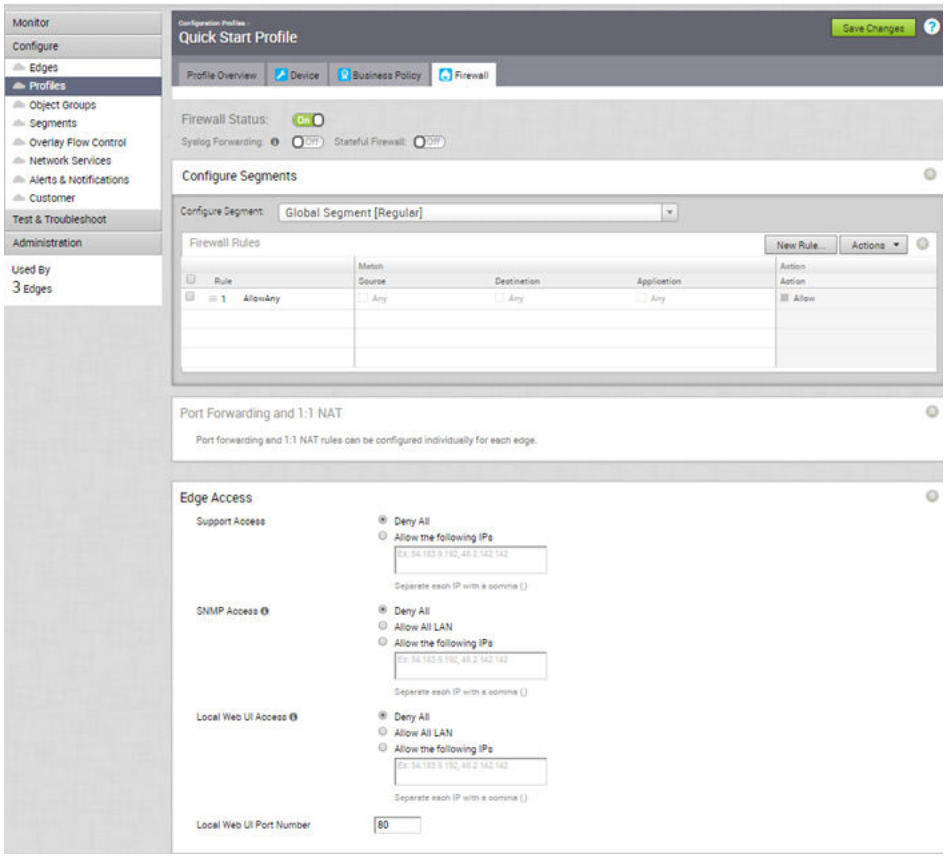
Dieses Kapitel enthält die folgenden Themen:

Konfigurieren der Firewall für Profile

Als Unternehmensadministrator können Sie Firewallregeln und Informationen zum Edge-Zugriff konfigurieren sowie den Firewallstatus und die Protokolle mithilfe der Registerkarte **Firewall** im Dialogfeld **Profilkonfiguration (Profile Configuration)** aktivieren oder deaktivieren.

Firewallprofile sind segmentierfähig. Alle Segmente, die für die Konfiguration verfügbar sind, werden im Dropdown-Menü **Segment konfigurieren (Configure Segment)** aufgelistet. Wenn Sie ein zu konfigurierendes Segment aus dem Dropdown-Menü **Segment konfigurieren (Configure Segment)** auswählen, werden die mit diesem Segment verknüpften Einstellungen und Optionen im Bereich **Segmente konfigurieren (Configure Segments)** angezeigt. **Globales Segment [Normal] (Global Segment [Regular])** ist das Standardsegment.

Weitere Informationen zur Segmentierung finden Sie unter Kapitel 7 Konfigurieren von Segmenten.



Die Firewall-Konfiguration auf der Profilebene umfasst:

- Aktivieren der Syslog-Weiterleitung. Standardmäßig ist die Funktion „Syslog-Weiterleitung (Syslog Forwarding)“ für ein Unternehmen deaktiviert. Um SD-WAN Orchestrator-gebundene Ereignisse und Firewallprotokolle zu erfassen, die vom Unternehmens-SD-WAN Edges stammen, und an eine oder mehrere zentrale Remote-Syslog-Collector-Instanzen (Server) weiterzuleiten, muss ein Unternehmensbenutzer diese Funktion auf Unternehmensebene aktivieren. Weitere Informationen zum Konfigurieren von Syslog Collector-Details pro Segment in der SD-WAN Orchestrator-Instanz finden Sie unter Konfigurieren von Syslog-Einstellungen auf der Profilebene.
- Aktivieren Sie die statusbehaftete Firewall auf der Profil- und Edge-Ebene. Standardmäßig ist die Funktion „Statusbehaftete Firewall (Stateful Firewall)“ für ein Unternehmen aktiviert. Um die statusbehaftete Firewallfunktion für ein Unternehmen zu deaktivieren, wenden Sie sich an einen Operator mit der Superuser-Berechtigung.
- Konfigurieren einer Firewallregel.
- Konfigurieren des Edge-Zugriffs

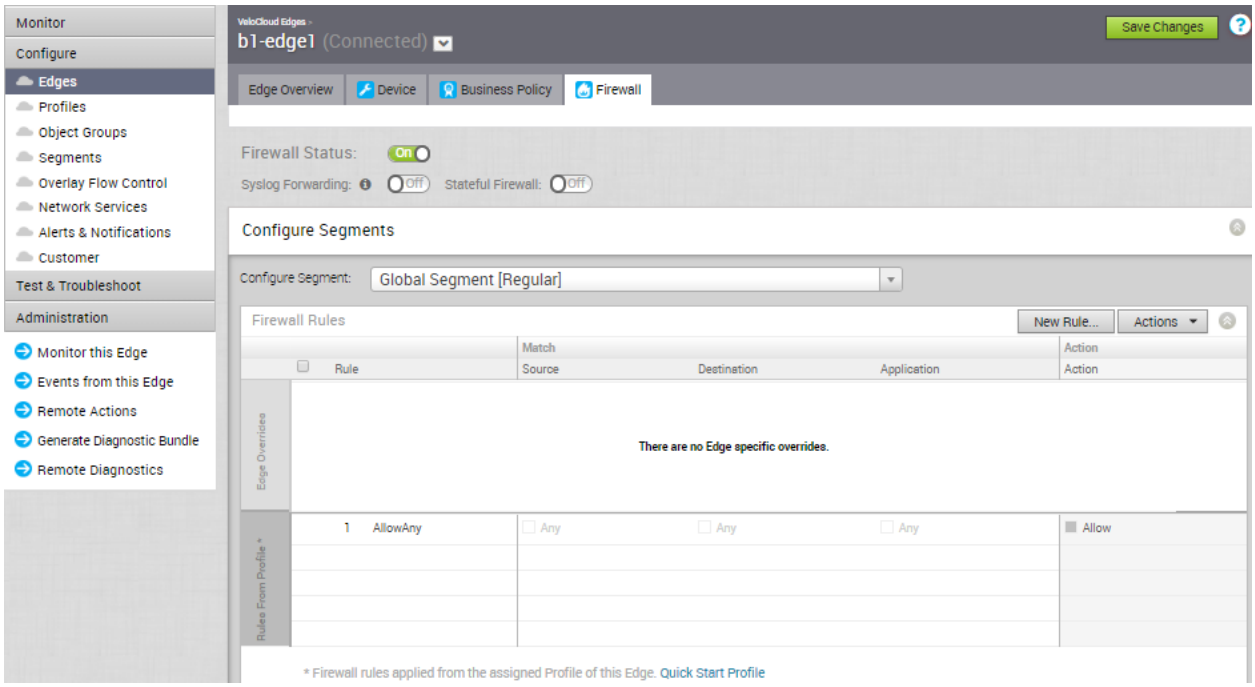
Hinweis Sie können die Firewallfunktion für Profile deaktivieren, indem Sie den **Firewallstatus (Firewall Status)** deaktivieren.

Verwandte Links

- Konfigurieren der Firewall für Edges
- Fehlerbehebung bei der Firewall

Konfigurieren der Firewall für Edges

Alle Edges erben die Firewallregeln und Edge Access-Konfigurationen vom zugehörigen Profil. Auf der Registerkarte **Firewall** im Dialogfeld **Edge-Konfiguration (Edge Configuration)** können Sie alle vererbten Firewallregeln im Bereich **Regel aus Profil (Rule From Profile)** anzeigen. Optional können Sie auf der Edge-Ebene auch die Profil-Firewall-Regeln und die Konfiguration des Edge-Zugriffs außer Kraft setzen.



Als Unternehmensadministrator können Sie die Portweiterleitung und 1:1-NAT-Firewallregeln für jeden Edge einzeln konfigurieren, indem Sie den Anweisungen auf dieser Seite folgen.

Portweiterleitung und 1:1-NAT-Firewallregeln

Hinweis Sie können die Portweiterleitung und 1:1-NAT-Regeln nur auf der Edge-Ebene individuell konfigurieren.

Portweiterleitung und 1:1-NAT-Firewallregeln ermöglichen Internet-Clients den Zugriff auf Server, die mit einer Edge-LAN-Schnittstelle verbunden sind. Der Zugriff kann entweder über Portweiterleitungsregeln oder 1:1-NAT (Network Address Translation)-Regeln bereitgestellt werden.

Portweiterleitungsregeln

Mit Portweiterleitungsregeln können Sie Regeln konfigurieren, um den Datenverkehr von einem bestimmten WAN-Port an ein Gerät (LAN-IP/LAN-Port) innerhalb des lokalen Subnetzes umzuleiten. Optional können Sie auch den eingehenden Datenverkehr durch eine IP-Adresse oder ein Subnetz einschränken. Das folgende Beispiel zeigt, wie die Portweiterleitungsregeln mit der externen IP konfiguriert werden (die sich im selben Subnetz der WAN-IP befindet).

Um eine Portweiterleitungsregel zu konfigurieren, geben Sie die folgenden Details an.

1 Geben Sie im Textfeld **Name** einen Namen (optional) für die Regel ein.

2 Wählen Sie im Dropdown-Menü **Protokoll (Protocol)** entweder TCP oder UDP als Protokoll für die Portweiterleitung aus.

3 Wählen Sie im Dropdown-Menü **Schnittstelle (Interface)** die Schnittstelle für den eingehenden Datenverkehr aus.

4 Geben Sie im Textfeld **Externe IP (Outside IP)** die IP-Adresse ein, über die auf den Host (Anwendung) vom externen Netzwerk aus zugegriffen werden kann.

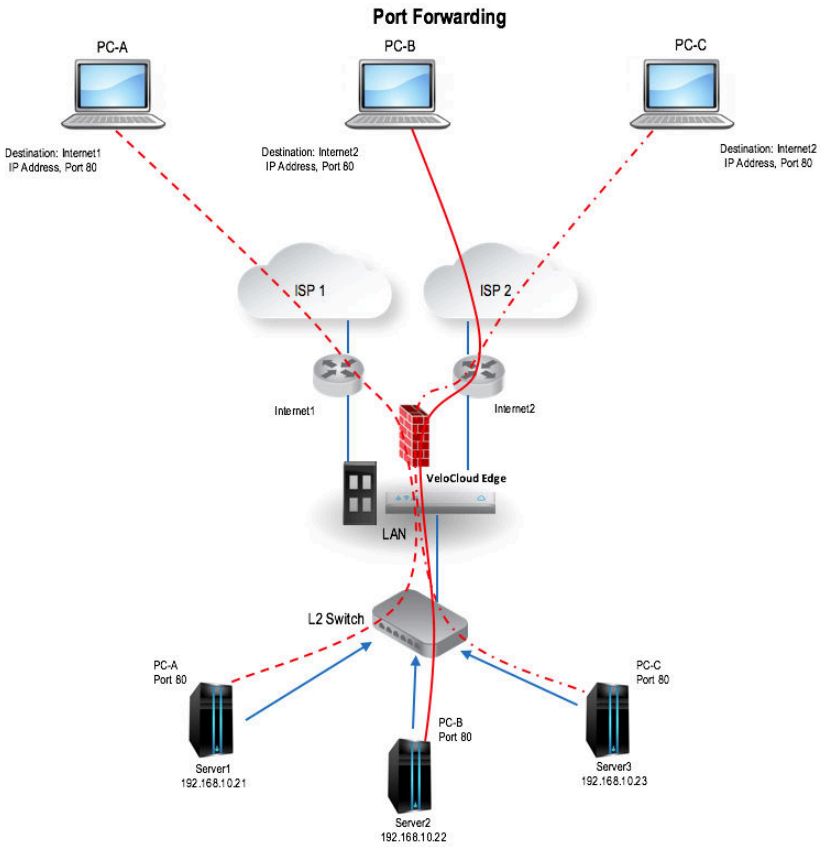
5 Geben Sie im Textfeld „WAN-Ports (WAN Ports)“ einen WAN Port oder einen Portbereich ein, der durch einen Bindestrich (-) getrennt ist, z. B. 20-25.

6 Geben Sie in den Textfeldern **LAN-IP (LAN IP)** und **LAN-Port (LAN Port)** die IP-Adresse und Portnummer des LAN ein, in dem die Anforderung weitergeleitet wird.

7 Wählen Sie im Dropdown-Menü **Segment** ein Segment aus, zu dem die LAN-IP gehören soll.

8 Geben Sie im Textfeld **Remote-IP/Subnetz (Remote IP/subnet)** eine IP-Adresse des eingehenden Datenverkehrs an, der an einen internen Server weitergeleitet werden soll. Wenn Sie keine IP-Adresse angeben, wird jeder Datenverkehr zugelassen.

Die folgende Abbildung veranschaulicht die Portweiterleitungskonfiguration.



1:1-NAT-Einstellungen

Diese werden verwendet, um eine externe IP-Adresse, die vom SD-WAN Edge unterstützt wird, einem Server zuzuordnen, der mit einer Edge-LAN-Schnittstelle verbunden ist (z. B. einem Webserver oder einem Mailserver). Eine 1:1-NAT-Zuordnung kann nur mit IP-Adressen konfiguriert werden, die nicht zum SD-WAN Edge gehören. Es können auch externe IP-Adressen in anderen Subnetzen als der WAN-Schnittstellenadresse übersetzt werden, wenn der Internetdienstanbieter den Datenverkehr für das Subnetz in Richtung SD-WAN Edge leitet. Jede Zuordnung erfolgt zwischen einer IP-Adresse außerhalb der Firewall für eine bestimmte WAN-Schnittstelle und einer LAN-IP-Adresse innerhalb der Firewall. Innerhalb jeder Zuordnung können Sie angeben, welche Ports an die interne IP-Adresse weitergeleitet werden. Das Symbol **'+'** auf der rechten Seite kann verwendet werden, um zusätzliche 1:1-NAT-Einstellungen hinzuzufügen.

Um eine 1:1-NAT-Regel zu konfigurieren, geben Sie die folgenden Details an.

1 Geben Sie im Textfeld **Name** einen Namen für die Regel ein.

2 Geben Sie im Textfeld **Externe IP (Outside IP)** die IP-Adresse ein, auf die der Host von einem externen Netzwerk aus zugreifen kann.

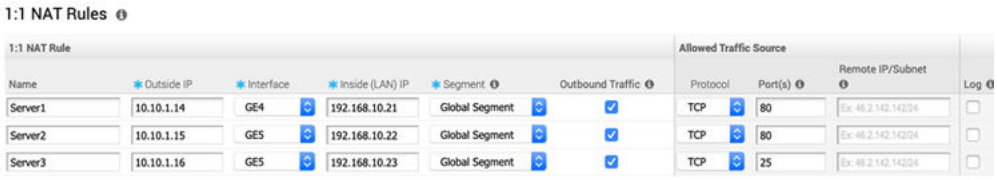
3 Wählen Sie im Dropdown-Menü **Schnittstelle (Interface)** die WAN-Schnittstelle aus, an die die externe IP-Adresse gebunden werden soll.

4 Geben Sie im Textfeld **Interne (LAN-)IP (Inside (LAN) IP)** die tatsächliche IP (LAN)-Adresse des Hosts ein.

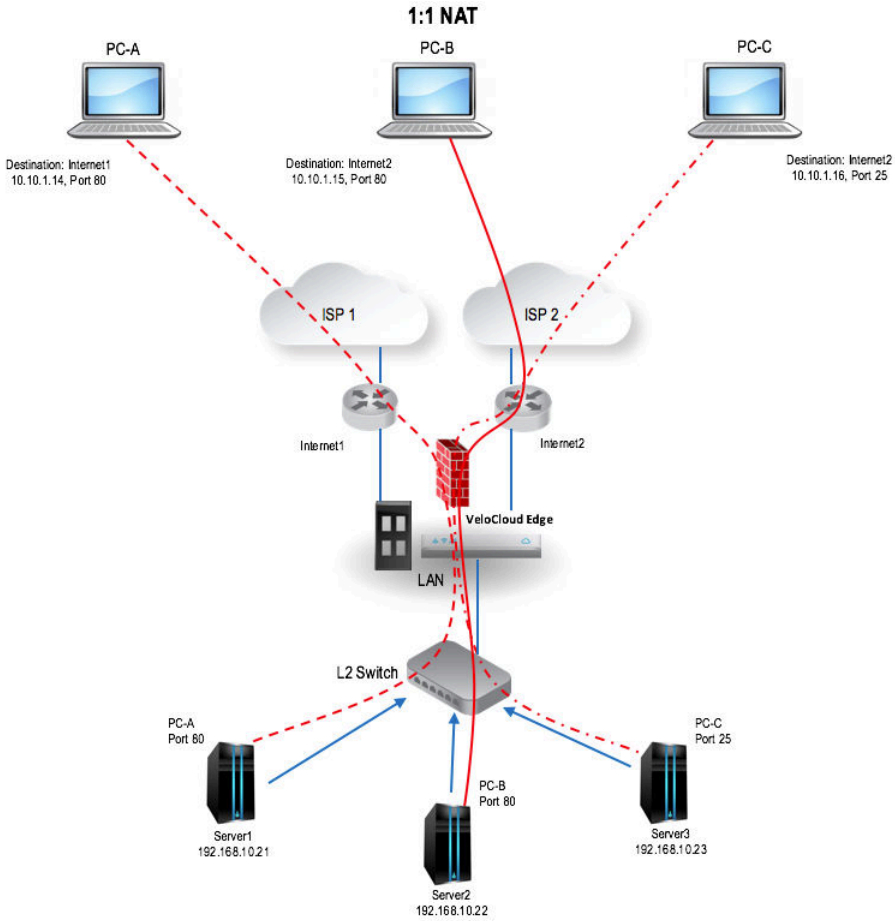
5 Wählen Sie im Dropdown-Menü **Segment** ein Segment aus, zu dem die LAN-IP gehören soll.

6 Aktivieren Sie das Kontrollkästchen **Ausgehender Datenverkehr (Outbound Traffic)**, wenn Sie dem ausgehenden Verkehr, der vom Internet zum LAN-Client an den Edge weitergeleitet wird, erlauben möchten, die Firewall-Verbindung zu passieren.

7 Geben Sie die Details der zulässigen Datenverkehrsquelle (Protokoll, Ports, Remote-IP/Subnetz) für die Zuordnung in die entsprechenden Felder ein.



Die folgende Abbildung veranschaulicht die 1:1-NAT-Konfiguration.



Konfigurieren von Edge-Außerkraftsetzungen

Optional können Sie auf der Edge-Ebene die Firewallregeln für das geerbte Profil außer Kraft setzen. Um Firewallregeln auf der Edge-Ebene außer Kraft zu setzen, klicken Sie unter **Firewallregeln (Firewall Rules)** auf **Neue Regel (New Rule)** und führen Sie die Schritte unter Konfigurieren einer Firewallregel aus. Die Außerkraftsetzungsregeln werden im Bereich **Edge-Außerkraftsetzungen (Edge Overrides)** angezeigt. Die Regeln für die Edge-Außerkraftsetzung haben Vorrang vor den vererbten Profilregeln für den Edge. Jeder Übereinstimmungswert für die Edge-Außerkraftsetzung, der mit einer Profil-Firewall-Regel übereinstimmt, setzt diese Profilregel außer Kraft.

Konfigurieren von Außerkraftsetzungen für den Edge-Zugriff

Optional können Sie auf der Edge-Ebene auch die Konfiguration des Edge-Zugriffs außer Kraft setzen. Um den Edge-Zugriff außer Kraft zu setzen, aktivieren Sie das Kontrollkästchen **Edge-Außerkraftsetzung aktivieren (Enable Edge Override)** im Bereich **Edge-Zugriff (Edge Access)** der Seite **Edge-Firewall (Edge Firewall)**. Weitere Informationen finden Sie unter Konfigurieren des Edge-Zugriffs.

Verwandte Links

- Konfigurieren der Firewall für Profile
- Konfigurieren von Syslog-Einstellungen auf der Edge-Ebene
- Fehlerbehebung bei der Firewall

Konfigurieren einer Firewallregel

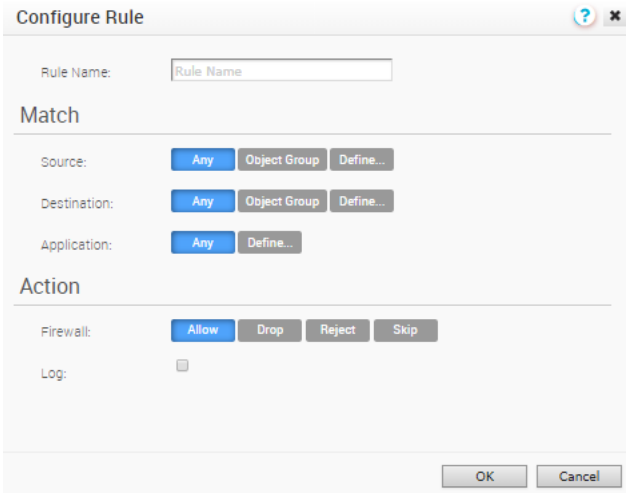
Mit SD-WAN Orchestrator können Sie Firewallregeln auf Profil- und Edge-Ebene konfigurieren, um ein- und ausgehenden Datenverkehr zuzulassen, zu löschen, abzulehnen oder zu überspringen. Die Firewall verwendet die Parameter wie Quell-IP-Adresse/Port, Ziel-IP-Adresse/Port, Anwendungen, Anwendungskategorien und DSCP-Tags, um Firewallregeln zu erstellen.

Um eine Firewallregel mit statusbehafteten Firewallregeln auf der Profilebene zu konfigurieren, führen Sie die Schritte in diesem Verfahren aus.

Verfahren

1. Navigieren Sie in SD-WAN Orchestrator zu **Konfigurieren (Configure)** > **Profile (Profiles)** > **Firewall**.
2. Aktivieren Sie **Statusbehaftete Firewall (Stateful Firewall)** für das ausgewählte Profil.

3 Klicken Sie im Bereich **Firewallregeln (Firewall Rules)** auf **Neue Regel (New Rule)**. Das Dialogfeld **Regel konfigurieren (Configure Rule)** wird angezeigt.



4 Geben Sie im Feld **Regelname (Rule Name)** einen eindeutigen Namen für die Regel ein.

5 Konfigurieren Sie im Bereich **Übereinstimmung (Match)** die Übereinstimmungsbedingungen für die Regel:

Einstellungen	Beschreibung
Quelle (Source)	Ermöglicht die Angabe der Quelle für Pakete. Wählen Sie eine der folgenden Optionen aus: ■ **Alle (Any)**: Erlaubt standardmäßig alle Quelladressen. ■ **Objektgruppe (Object Group)**: Sie können eine Kombination aus Adressgruppe und Portgruppe auswählen. ■ **Definieren (Define)**: Ermöglicht die Definition des Quelldatenverkehrs zu einem bestimmten VLAN, einer IP-Adresse, einer MAC-Adresse oder einem Port. Für IP-Adresse wählen Sie eine der drei Optionen aus: ■ **CIDR-Präfix (CIDR prefix)**: Wählen Sie diese Option aus, wenn das Netzwerk als Wert für CIDR definiert werden soll (z. B: `172.10.0.0 /16`). ■ **Subnetzmaske (Subnet mask)**: Wählen Sie diese Option aus, wenn das Netzwerk basierend auf einer Subnetzmaske definiert werden soll (z. B. `172.10.0.0 255.255.0.0`). ■ **Platzhaltermaske (Wildcard mask)**: Wählen Sie diese Option aus, wenn Sie die Durchsetzung einer Richtlinie auf eine Reihe von Geräten für verschiedene IP-Subnetze beschränken möchten, die einen übereinstimmenden Wert für die IP-Adresse des Hosts verwenden. Die Platzhaltermaske entspricht einer IP oder einer Reihe von IP-Adressen, die auf der umgekehrten Subnetzmaske basieren. Eine '0' innerhalb des Binärwerts der Maske bedeutet, dass der Wert „fest“ ist, und eine 1 innerhalb des Binärwerts der Maske bedeutet, dass der Wert „variabel“ ist (kann 1 oder 0 sein). Beispiel: eine Platzhaltermaske von 0.0.0.255 (binäres Äquivalent = 00000000.00000000.00000000.11111111) mit einer IP-Adresse von 172.0.0, wobei die ersten drei Oktette feste Werte sind und das letzte Oktett ein variabler Wert ist.
Ziel (Destination)	Ermöglicht die Angabe des Ziels für Pakete. Wählen Sie eine der folgenden Optionen aus: ■ **Alle (Any)**: Erlaubt standardmäßig alle Zieladressen. ■ **Objektgruppe (Object Group)**: Sie können eine Kombination aus Adressgruppe und Portgruppe auswählen. Weitere Informationen zur Objektgruppe finden Sie unter Kapitel 17 Objektgruppen. ■ **Definieren (Define)**: Ermöglicht die Definition des Zieldatenverkehrs zu einem bestimmten VLAN, einer IP-Adresse, einer Mac-Adresse oder einem Port. Für

Einstellungen	Beschreibung
	die IP-Adresse wählen Sie eine der drei Optionen aus: **CIDR-Präfix (CIDR Prefix)**, **Subnetzmaske (Subnet mask)** oder **Platzhaltermaske (Wildcard mask)**.
Anwendung (Application)	Ermöglicht das Angeben der Anwendungen, auf die die Firewallregel angewendet werden soll. Wählen Sie eine der folgenden Optionen aus: ■ **Alle (Any)**: Wendet die Firewallregel standardmäßig auf alle Anwendungen an. ■ **Definieren (Define)**: Ermöglicht Ihnen die Auswahl einer bestimmten Anwendung.

6 Konfigurieren Sie im Bereich **Aktion (Action)** die Aktionen für die Regel:

Einstellungen	Beschreibung
Firewall	Wählen Sie eine der folgenden Aktionen aus, die die Firewall bei Paketen ausführen soll, wenn die Bedingungen der Regel erfüllt sind: ■ **Zulassen (Allow)**: Lässt die Datenpakete standardmäßig zu. ■ **Löschen (Drop)**: Löscht die Datenpakete stillschweigend, ohne eine Benachrichtigung an die Quelle zu senden. ■ **Ablehnen (Reject)**: Löscht die Pakete und benachrichtigt die Quelle durch Senden einer expliziten Wiederherstellungsnachricht. ■ **Überspringen (Skip)**: Überspringt die Regel bei Lookups und verarbeitet die nächste Regel. Diese Regel wird jedoch zum Zeitpunkt der Bereitstellung von SD-WAN verwendet.
Protokoll (Log)	Aktivieren Sie dieses Kontrollkästchen, wenn Sie möchten, dass beim Auslösen dieser Regel ein Protokolleintrag erstellt wird.

7 Klicken Sie auf **OK**.

Ergebnisse

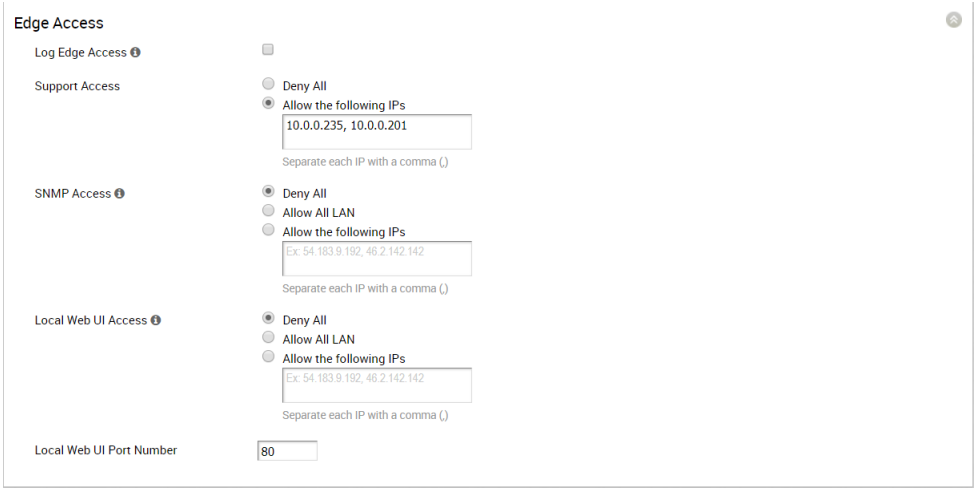
Eine Firewallregel wird für das ausgewählte Profil erstellt und auf der Seite **Profil-Firewall (Profile Firewall)** im Bereich **Firewallregeln (Firewall Rules)** angezeigt.

Konfigurieren des Edge-Zugriffs

Wenn Sie ein Profil für den Edge-Zugriff konfigurieren, müssen Sie sicherstellen, dass Sie in den Firewall-Einstellungen die entsprechende Option für den Support-Zugriff, den SNMP-Zugriff und den lokalen Web-UI-Zugriff auswählen. Standardmäßig sind die Optionen für den Support-Zugriff, den SNMP-Zugriff und den lokalen Web-UI-Zugriff aus Sicherheitsgründen deaktiviert.

Verfahren

1 Navigieren Sie in SD-WAN Orchestrator zu **Konfigurieren (Configure)** > **Profile (Profiles)** > **Firewall**.



2 Aktivieren Sie unter **Edge-Zugriff (Edge Access)** das Kontrollkästchen **Edge-Zugriff protokollieren (Log Edge Access)**, um jeden Edge-Zugriff zu protokollieren.

3 Wählen Sie für **Supportzugriff (Support Access)** die Option **Die folgenden IPs zulassen (Allow the following IPs)** aus und geben Sie explizit die IP-Adressen an, von denen aus Sie SSH auf diesem Edge einleiten können.

4 Wählen Sie für den **SNMP-Zugriff (SNMP Access)** von der gerouteten Schnittstelle/WAN die Option **Alle LANs zulassen (Allow All LAN)** oder **Die folgenden IPs zulassen (Allow the following IPs)** aus, wenn sich die SNMP-Server im LAN befinden.

5 Wählen Sie für den **Lokalen Web-UI-Zugriff (Local Web UI Access)** von der gerouteten Schnittstelle/WAN die Option **Alle LANs zulassen (Allow All LAN)** oder **Die folgenden IPs zulassen (Allow the following IPs)** aus.

6 Geben Sie im Textfeld **Portnummer der lokalen Web-UI (Local Web UI Port Number)** die Portnummer der lokalen Web-UI ein.

7 Klicken Sie auf **Änderungen speichern (Save Changes)**.

Ergebnisse

Nächste Schritte

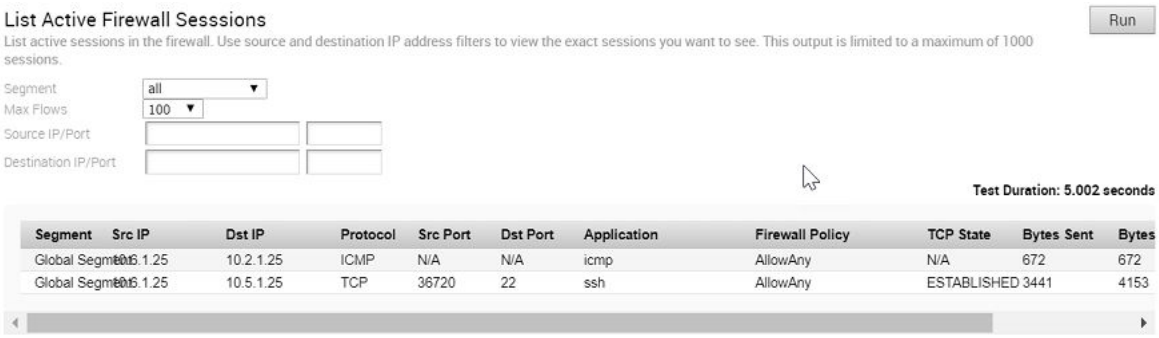
Wenn Sie die Einstellungen für den Edge-Zugriff für einen bestimmten Edge außer Kraft setzen möchten, verwenden Sie die Option **Edge-Außerkraftsetzung aktivieren (Enable Edge Override)**, die auf der Seite **Edge-Firewall (Edge Firewall)** verfügbar ist. Weitere Informationen finden Sie unter Konfigurieren der Firewall für Edges

Fehlerbehebung bei der Firewall

Sie können die Firewalldiagnoseprotokolle erfassen, indem Sie die Remote-Diagnosetests auf einem Edge ausführen.

Die folgenden Remote-Diagnosetests werden zum Abrufen der Firewalldiagnoseinformationen verwendet:

- **Liste der aktiven Firewallsitzungen (List Active Firewall Sessions)**: Listet aktive Sitzungen in der Firewall auf, wie im folgenden Screenshot dargestellt.



- **Firewallsitzungen leeren (Flush Firewall Sessions)**. Setzt eingerichtete Sitzungen der Firewall zurück.

Weitere Informationen zur Ausführung der Remote-Diagnose auf einem Edge finden Sie unter Remote-Diagnose.

Erstellen oder Auswählen eines Netzwerks

13

Führen Sie die Schritte in diesem Verfahren durch, um ein Netzwerk zu konfigurieren:

Hinweis Wenn Sie mit einer Benutzer-ID angemeldet sind, die über Kundensupport-Berechtigungen verfügt, können Sie nur SD-WAN Orchestrator-Objekte anzeigen. Sie werden nicht in der Lage sein, neue Objekte zu erstellen oder bestehende zu konfigurieren/aktualisieren.

Netzwerkkonfiguration

1 Erstellen eines neuen Netzwerks oder Auswählen eines vorhandenen Netzwerks

2 Konfigurieren von Unternehmensnetzwerken

   a Konfigurieren des Adressraums

   b Konfigurieren von VLANs

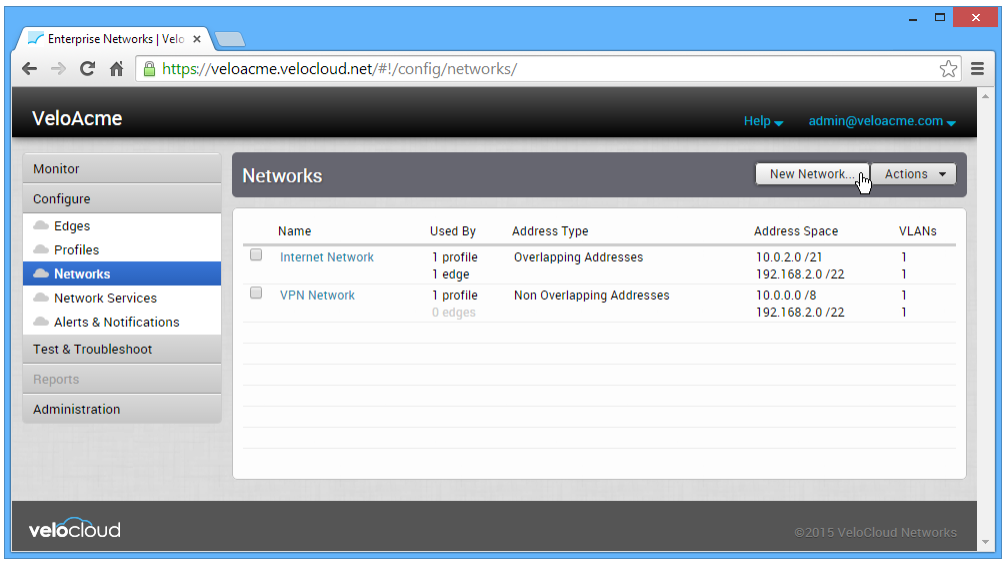
3 Konfigurieren von Gastnetzwerken

   a Konfigurieren des Adressraums

   b Konfigurieren von VLANs

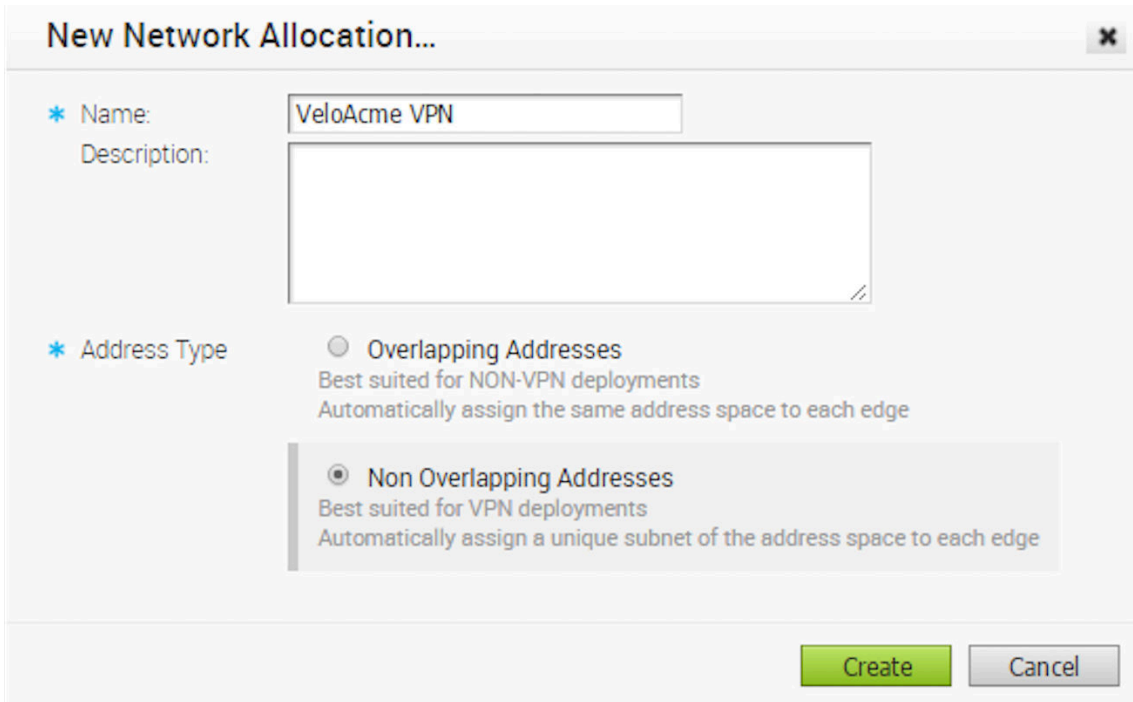
Erstellen eines Netzwerks oder Auswählen eines vorhandenen Netzwerks

Wenn Sie ein neues Netzwerk erstellen, klicken Sie auf der Seite **Netzwerke (Networks)** auf **Neues Netzwerk (New Network)**. Alternativ können Sie ein vordefiniertes Netzwerk auswählen, indem Sie auf den Namen des vordefinierten Netzwerks klicken. Nach einer neuen Installation verfügt die SD-WAN Orchestrator-Instanz über zwei vordefinierte Netzwerke: Internet-Netzwerk und VPN-Netzwerk.



Wenn Sie ein neues Netzwerk erstellen, wird das Dialogfeld **Neue Netzwerkzuteilung (New Network Allocation)** angezeigt (siehe Bild unten). Geben Sie im Dialogfeld **Neue Netzwerkzuteilung (New Network Allocation)** einen Namen und eine Beschreibung ein und wählen Sie einen Adresstyp aus.

Obwohl der Adresstyp entweder überlappende Adressen (jeder SD-WAN Edge verfügt über denselben Adressbereich) oder keine überlappenden Adressen (jeder SD-WAN Edge verfügt über einen eindeutigen Adressblock) aufweist, legen wir „Keine Überlappung (Non Overlapping)“ fest. In diesem Beispiel rufen wir unser neues Netzwerk namens „VeloAcme VPN“ auf.



Überlappende Adressen

Damit Zweige mit überlappender IP den gemeinsamen Server im Hub oder Datencenter erreichen können oder damit Datencenter-Benutzer Server in Zweigstellen mit überlappender IP erreichen können, muss NAT auf dem Edge konfiguriert werden. Sie können NAT für eine einzelne lokale Quell-IP definieren, um sie einer VPN-IP-Adresse zuzuordnen, oder für einen Block von IP-Adressen auf einen Block von VPN-Adressen mit derselben Präfixlänge.

Es sind zwei Schritte erforderlich, die Sie abschließen müssen:

1 Aktivieren Sie VPN über NAT im Setup für das überlappende Adressnetzwerk.

2 *Konfigurieren Sie NAT auf der Edge-Ebene*.

Siehe nachstehende Anweisungen zur Konfiguration der überlappenden IP-Adresse für VPN.

Konfigurieren von überlappenden IP-Adressen für VPN

So konfigurieren Sie überlappende IP-Adressen für VPN:

1 Aktivieren Sie VPN über NAT im Setup für das überlappende Adressnetzwerk.

   a Navigieren Sie im Navigationsbereich zu **Konfigurieren (Configure) > Netzwerke (Networks)**.

   b Klicken Sie auf die Schaltfläche **Neues Netzwerk (New Network)**.

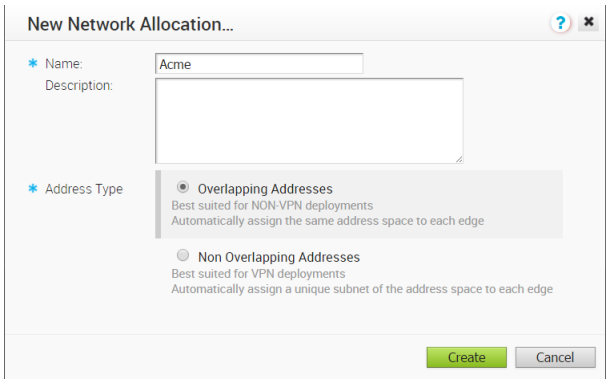
   c Gehen Sie im Dialogfeld **Neue Netzwerkzuteilung (New Network Allocation)** wie folgt vor:

      1 Geben Sie den Netzwerknamen in das Textfeld **Name** ein.

      2 Wenn eine Beschreibung vorliegt, geben Sie sie in das Textfeld **Beschreibung (Description)** ein.

      3 Wählen Sie im Bereich **Adresstyp (Address Type)** die Option **Überlappende Adressen (Overlapping Addresses)** aus.

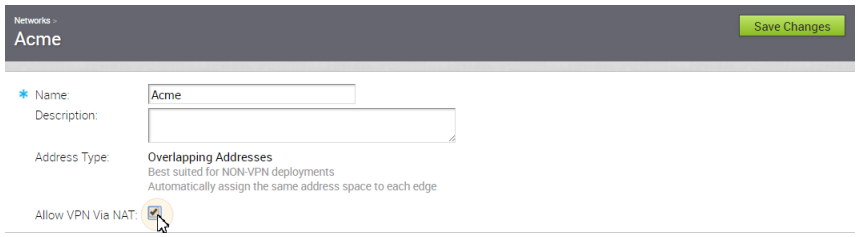
      4 Klicken Sie auf die Schaltfläche **Erstellen (Create)**.



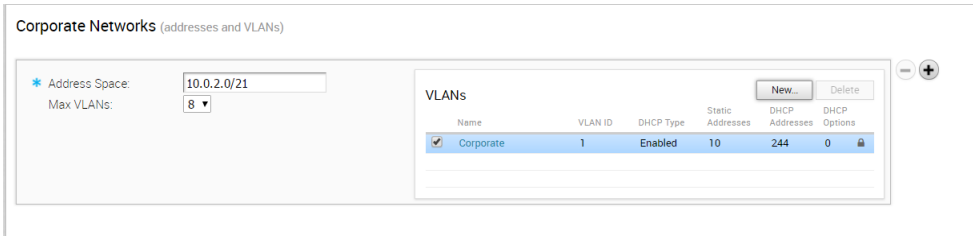
   d Klicken Sie auf den neu erstellten Netzwerklink im Bildschirm **Netzwerk (Network)**.

e Aktivieren Sie im Bildschirm **Netzwerke (Networks)** das Kontrollkästchen **VPN über NAT zulassen (Allow VPN Via NAT)**, wenn NAT auf dem Edge erforderlich ist. Siehe Abbildung unten.

f Klicken Sie auf die Schaltfläche **Änderungen speichern (Save Changes)**.



2 Erstellen Sie im Bereich **Unternehmensnetzwerke (Corporate Networks)** ein neues VLAN oder aktualisieren Sie ein vorhandenes VLAN.

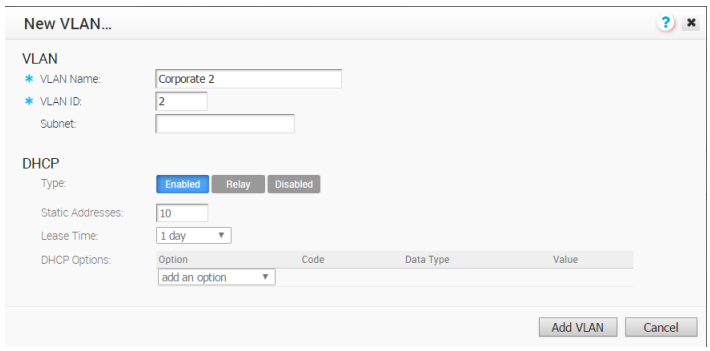


a Wenn Sie ein vorhandenes VLAN aktualisieren, klicken Sie auf den VLAN-Link, um das Dialogfeld **Unternehmen (Corporate)** zu öffnen.

b Wenn Sie ein neues VLAN erstellen, klicken Sie auf die Schaltfläche **Neu (New)** im Bereich **VLANs**, um das Dialogfeld **Neues VLAN (New VLAN)** zu öffnen. (Geben Sie im Dialogfeld **Neues VLAN (New VLAN)** den VLAN-Namen unter **VLAN-Name (VLAN Name)** und die **VLAN-ID (VLAN ID)** ein.)

c Geben Sie im Textfeld **Subnetz (Subnet)** das Subnetz ein.

d Klicken Sie auf die Schaltfläche **VLAN hinzufügen (Add VLAN)**.



3 Definieren Sie bei Aktivierung der Option **VPN über NAT zulassen (Allow VPN Via NAT)** NAT auf der Edge-Ebene (1:1 oder verwenden Sie VPN-IP-Subnetz-Blockpool). Weitere Informationen finden Sie im Abschnitt *Konfigurieren des Edge-Geräts*.

Nicht überlappende Adressierung

Die Zusammenfassung des neuen Netzwerks, in dem sich eine nicht überlappende Adressierung befindet, wird in der folgenden Bildschirmaufnahme angezeigt. In dieser Netzwerkdefinition verfügt jeder Edge über einen eindeutigen Netzwerkadressraum. VeloAcme verfügt auch über einige Edges, die eine Kommunikation zwischen den Edges mithilfe eines VPN-Tunnel erfordern. Dies setzt voraus, dass jede Verbindung über alle Edges eine eindeutige IP-Adresse aufweisen muss.

VMware SD-WAN Site-VPN

Unternehmensnetzwerk konfigurieren (Configure Corporate Network)

Hinweis Anfänglich ist ein Unternehmensnetzwerk definiert. Zusätzliche Unternehmensnetzwerke können durch Klicken auf das Plus-Symbol (+) rechts neben dem Netzwerk definiert werden.

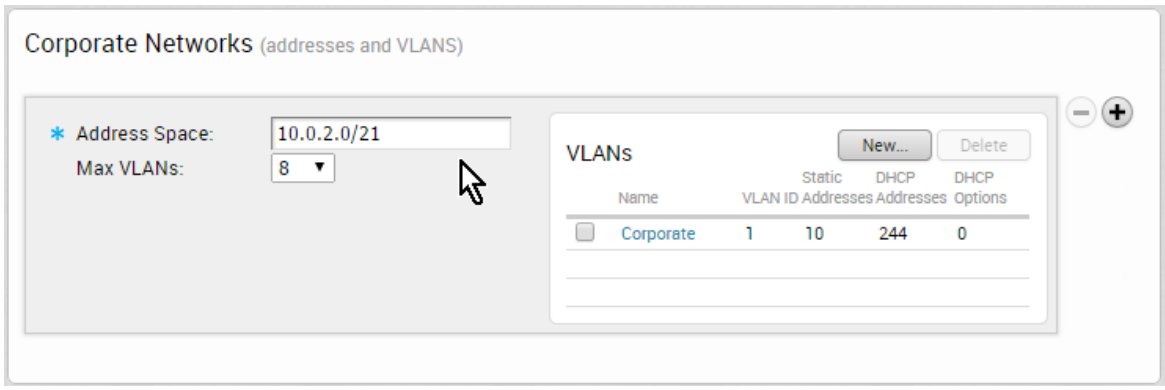
Führen Sie die folgenden Schritte für Ihr VPN-Unternehmensnetzwerk aus.

Konfigurieren des Adressraums

Geben Sie den Adressbereich für das Unternehmensnetzwerk ein.

SaaS

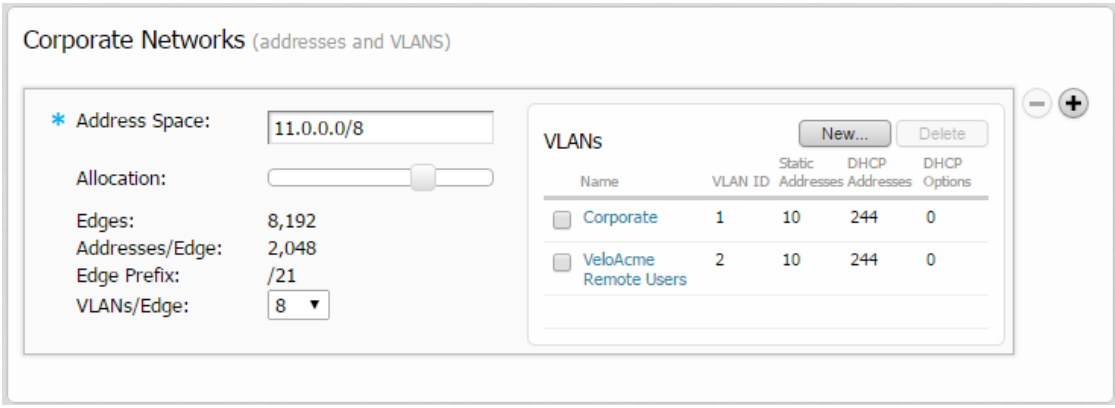
Die folgende Bildschirmaufnahme zeigt ein Unternehmensnetzwerk, das eine überlappende Adressierung verwendet. Geben Sie den Adressbereich ein, den das Unternehmensnetzwerk auf allen Edges belegen wird.



Hinweis Obwohl SaaS für VPN verwendet werden kann, legen wir „Keine Überlappung (Non-Overlapping)“ fest.

Non VMware SD-WAN Site über VPN

Das folgende Bild zeigt ein Unternehmensnetzwerk, das eine überlappende Adressierung verwendet. Der Adressraum wurde im vorherigen Schritt bei der Erstellung des Netzwerkbereichs festgelegt und wird über die Anzahl der mit dem Zuweisungs-Schieberegler gewählten Edges verteilt. Sie können den Wert für „Edges“, „Adressen/Edge (Addresses/Edge)“ und das „Edge-Präfix (Edge Prefix)“ angeben. Der Zuweisungs-Schieberegler hilft Ihnen bei der Auswahl dieser Werte, indem er die Werte berechnet, wenn alle Adressen über die Anzahl der Edges hinweg zugewiesen werden. Hierbei handelt es sich um die integrierte IPAM-IP-Adressverwaltung für Edges zur Zuweisung von LAN-seitigen Subnetzen hinter dem Edge.



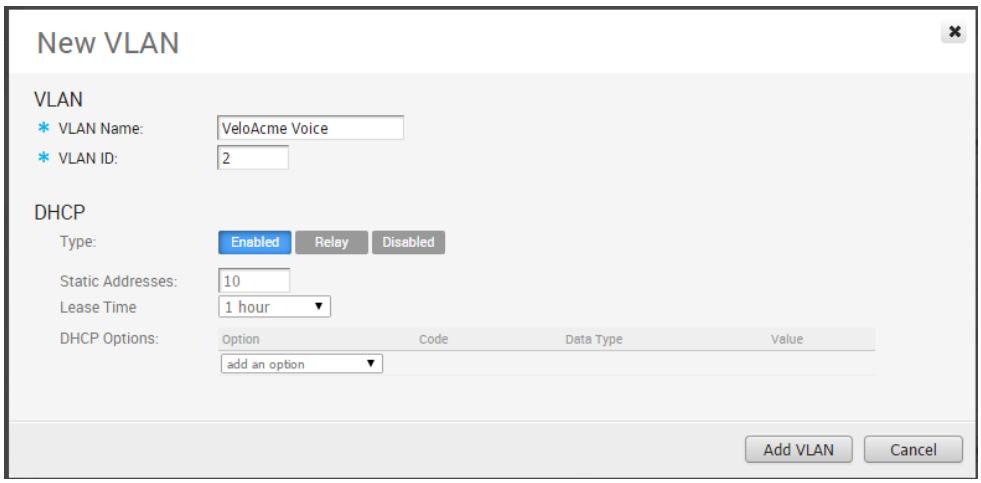
Hinweis Sobald ein Netzwerk einem Edge zugewiesen ist, ist es nicht mehr möglich, die Adressraumzuweisung zu ändern.

Hinweis Die Anzahl der Edges ist die maximale Anzahl von Edges, die jemals über dieses Netzwerk eingesetzt werden. „Adressen/Edge (Addresses/Edge)“ definiert die Größe des Adressraums für jeden Edge.

Konfigurieren von VLANs

Sie können für das Unternehmensnetzwerk beliebig viele VLANs definieren, der Wert „Maximale Anzahl von VLANs (Max VLANs)“ gibt jedoch die Höchstanzahl an, die Sie für die Verwendung in einem Profil oder Edge angeben können.

Klicken Sie auf die Schaltfläche „Neu (New)“, um ein neues VLAN zu erstellen. Sie können den VLAN-Namen, die VLAN-ID und die DHCP-Konfiguration konfigurieren.



Wählen Sie im Bereich **DHCP** einen der folgenden DHCP-Typen aus:

- **Aktiviert (Enabled)** – Aktiviert DHCP mit den Edges als DHCP-Server. Wenn Sie diese Option auswählen, müssen Sie die folgenden Details angeben:
  - **Statische Adressen (Static Addresses)** – Geben Sie die Anzahl der statischen IP-Adressen ein, die in einem Subnetz auf dem DHCP-Server zur Verfügung stehen.
  - **Lease-Dauer (Lease Time)** – Wählen Sie im Dropdown-Menü den Zeitraum aus, in dem das VLAN eine IP-Adresse verwenden kann, die dynamisch vom DHCP-Server zugewiesen wurde.

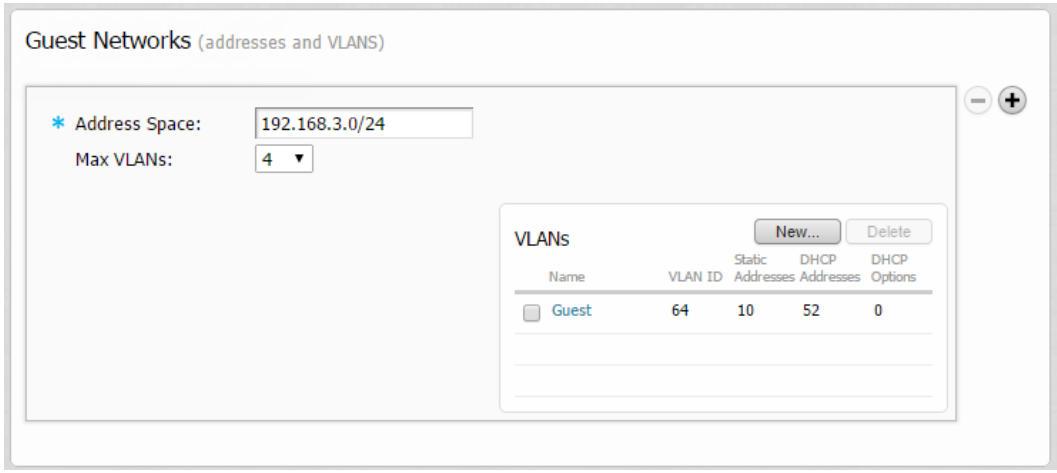
  Sie können auch eine oder mehrere DHCP-Optionen hinzufügen, wenn Sie vordefinierte Optionen angeben oder benutzerdefinierte Optionen hinzufügen.
- **Relay** – Aktiviert DHCP mit dem in einem Remote-Speicherort installierten DHCP-Relay-Agenten. Wenn Sie diese Option auswählen, können Sie die IP-Adresse eines oder mehrerer Relay-Agenten angeben.
- **Deaktiviert (Disabled)** – Deaktiviert DHCP.

Klicken Sie auf **VLAN hinzufügen (Add VLAN)**, um die VLAN-Erstellung abzuschließen.

Konfigurieren von Gastnetzwerken

Hinweis Anfänglich ist ein Gastnetzwerk definiert. Zusätzliche Gastnetzwerke können durch Klicken auf das Symbol „**+**“ rechts neben dem Netzwerk definiert werden.

Das Gastnetzwerk ist ein nicht vertrauenswürdiges Netzwerk, das immer einen überlappenden Adressraum verwendet. Es ist vollständig segmentiert und im Vergleich zum Unternehmensnetzwerk auf einem separaten VRF. Im Abschnitt **Gastnetzwerk (Guest Network)** (siehe Bildschirmaufnahme unten) wird der Adressraum definiert. Sie können beliebig viele VLANs für das Gastnetzwerk definieren, aber der Wert „Maximale Anzahl von VLANs (Max VLANs)“ gibt die maximale Anzahl an, die Sie in einem Profil oder Edge verwenden können.



Konfigurieren des Adressraums

Geben Sie den Adressraum ein, den das Gastnetzwerk auf allen Edges belegen wird.

Konfigurieren von VLANs

Sie können beliebig viele VLANs für das Gastnetzwerk definieren, aber der Wert „Maximale Anzahl von VLANs (Max VLANs)“ gibt die maximale Anzahl an, die Sie in einem Profil oder Edge verwenden können. Für VeloAcme wird das Standard-VLAN namens „Gast (Guest)“ verwendet.

Unsere VeloAcme-Netzwerkdefinitionen sind jetzt vollständig und können in unsere Profil- und Edge-Definitionen integriert werden.

Bereitstellen eines Edge

14

In diesem Abschnitt wird beschrieben, wie ein Edge bereitgestellt wird.

Dieses Kapitel enthält die folgenden Themen:

Bereitstellen eines neuen Edge

Enterprise-Administratoren können einen einzelnen Edge oder mehrere Edges bereitstellen, z. B. einem Edge eine Profilkonfiguration zuweisen oder andere Edge-spezifische Parameter ändern. Sie müssen eine Konfiguration für jeden Edge erstellen, den Sie für eine bestimmte Site bereitstellen.

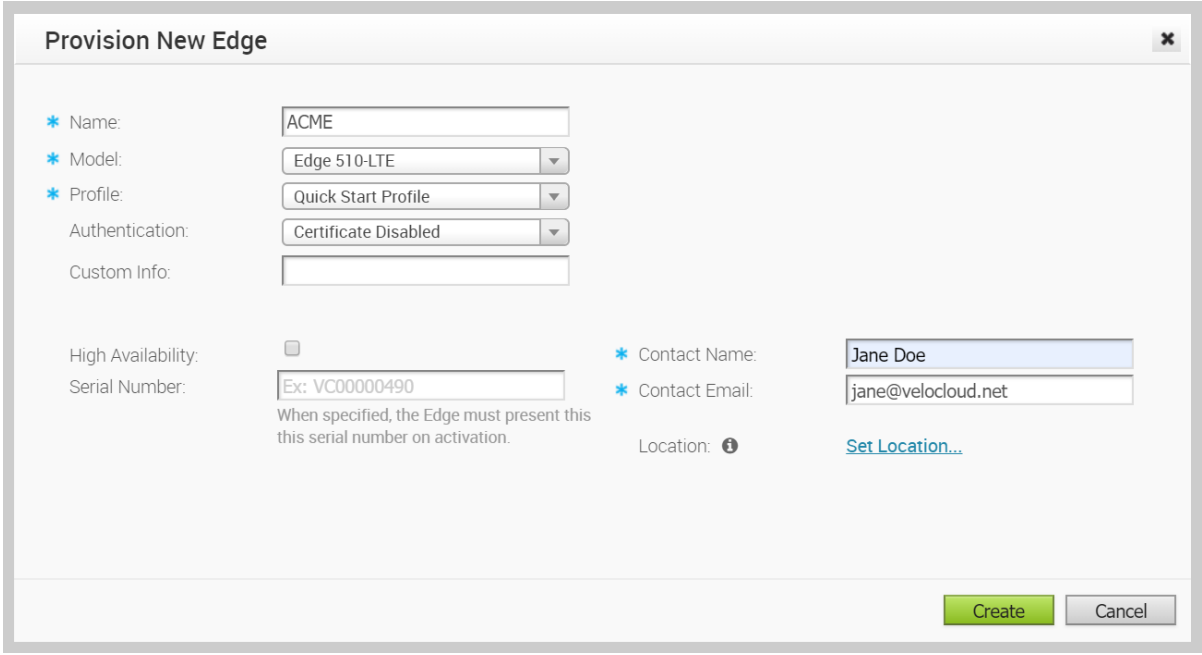
Sie können einen neuen Edge über den Bildschirm **Edges** bereitstellen, indem Sie die folgenden Schritte ausführen:

Verfahren

1 Klicken Sie im Unternehmensportal auf **Konfigurieren (Configure)** > **Edges**.

2 Klicken Sie im Bildschirm **Edges** oben rechts auf **Neuer Edge (New Edge)**.

Das Dialogfeld **Neuen Edge bereitstellen (Provision New Edge)** wird angezeigt.



3 Geben Sie im Textfeld **Name** einen eindeutigen Namen für den Edge ein.

4 Wählen Sie im Dropdown-Menü **Modell (Model)** ein Edge-Modell aus.

Hinweis Ab Version 3.4 wird Edge 510-LTE unterstützt und kann bereitgestellt werden.

5 Wählen Sie im Dropdown-Menü **Profil (Profile)** ein Profil aus, das dem Edge zugewiesen werden soll.

- Wenn aufgrund der Aktivierung per Push ein Edge-Staging-Profil als Option angezeigt wird, wird dieses Profil von einem neu zugewiesenen Edge verwendet, wurde aber nicht mit einem Produktionsprofil konfiguriert.
- Wenn ein Kunde über ein netzwerkbasiertes Operator-Profil verfügt, kann der Kunde nur netzwerkbasierte Edges bereitstellen. Wenn ein Kunde außerdem über ein segmentbasiertes Operator-Profil verfügt, kann der Kunde nur segmentbasierte Edges bereitstellen. (Weitere Informationen zur Profilmigration finden Sie unter Migration von Netzwerk zu Segment. Weitere Informationen zum Erstellen eines neuen Profils finden Sie im Kapitel 9 Konfigurieren von Profilen im Abschnitt Erstellen eines Profils.

6 Wählen Sie im Dropdownmenü **Authentifizierung (Authentication)** eine der folgenden Optionen aus: **Zertifikat deaktiviert (Certificate Disabled)**, **Zertifikat optional (Certificate Optional)** und **Zertifikat erforderlich (Certificate Required)** für die zertifikatbasierte Authentifizierung.

7 Geben Sie im Textfeld **Benutzerdefinierte Info (Custom Info)** benutzerdefinierte Informationen ein, die dem Edge zugeordnet sind

. Kundendaten dürfen nicht länger als 255 Zeichen sein.

Hinweis Die Benutzer „Superuser“ und „Standard-Admin“ der Rollen „Enterprise/MSP/ Operator“ (mit Berechtigung UPDATE_EDGE) können die benutzerdefinierten Informationen für einen Edge hinzufügen oder aktualisieren.

8 Um Hochverfügbarkeit (HA) anzuwenden, aktivieren Sie das Kontrollkästchen **Hochverfügbarkeit (High Availability)**. (Edges können als einzelnes eigenständiges Gerät installiert oder mit einem anderen Edge gekoppelt werden, um Hochverfügbarkeit (HA) zu unterstützen. Weitere Informationen zu HA finden Sie im Abschnitt Hochverfügbarkeitsoptionen.)

9 Geben Sie im Textfeld **Seriennummer (Serial Number)** die Seriennummer des Edge ein. Die angegebene Seriennummer muss der Seriennummer des Edge entsprechen, die aktiviert wird.

10 Geben Sie in die Textfelder **Kontaktname (Contact Name)** und **Kontakt-E-Mail-Adresse (Contact Email)** den Namen und die E-Mail-Adresse des Site-Kontakts für den Edge ein.

11 Klicken Sie auf den Link **Standort festlegen (Set Location)**, um den Standort des Edge festzulegen.

12 Klicken Sie auf **Erstellen (Create)**.

Ergebnisse

Der Edge wird mit einem Aktivierungsschlüssel bereitgestellt.

Hinweis Der Aktivierungsschlüssel läuft in einem Monat ab, wenn das Edge-Gerät nicht anhand des Schlüssels aktiviert wird. Informationen zum Aktivieren eines Edge finden Sie im Abschnitt Konfigurieren der Edge-Aktivierung in der *Kurzanleitung zur Edge-Aktivierung*.

Nächste Schritte

Nachdem Sie auf **Erstellen (Create)** geklickt haben, wird der Bildschirm **Edge-Übersicht (Edge Overview)** mit dem Edge-Aktivierungsschlüssel oben im Bildschirm angezeigt. Eine Übersicht über den soeben erstellten Edge oder Informationen dazu, wie Sie Änderungen daran vornehmen, finden Sie im Abschnitt Kapitel 15 Registerkarte „Edge-Übersicht (Edge Overview)“.

Nachdem Sie den Edge bereitgestellt haben, können Sie die folgenden Aktionen über das Dropdown-Menü **Aktionen (Actions)** ausführen:

- **Neuer Edge (New Edge)**: Erstellt einen neuen Edge.
- **Lokale Anmeldedaten (Local Credentials)**: Weisen Sie der lokalen Konfiguration Anmeldedaten für den ausgewählten Edge zu.
- **Edge löschen (Delete Edge)**: Löscht die ausgewählten Edges.
- **Profil zuweisen (Assign Profile)**: Ändern Sie das Profil für die ausgewählten Edges.

- **Operator-Profil zuweisen (Assign Operator Profile)**: Ändern Sie das Operator-Profil.

  Hinweis Diese Option ist nur für Operator-Benutzer verfügbar.

- **Vorabbenachrichtigungen aktualisieren (Update Pre-Notifications)**: Aktivieren oder deaktivieren Sie Edge-Warnungen und -Benachrichtigungen für Operatoren.
- **Edge-Lizenzierung (Edge Licensing)**: Weisen Sie einem ausgewählten Edge einen Lizenztyp zu.

  Hinweis Superuser-Administratoren und Standard-Administratoren können einem Edge einen Lizenztyp zuweisen.

- **Kundenwarnungen aktualisieren (Update Customer Alerts)**: Aktivieren oder deaktivieren Sie Edge-Warnungen und -Benachrichtigungen für Kunden.
- **Gateways neu ausgleichen (Rebalance Gateways)**: Bringen Sie SD-WAN-gehostete Gateways für den Enterprise-Edge wieder ins Gleichgewicht.

  Hinweis Diese Option ist nur für Operator-Benutzer verfügbar.

Weitere Informationen finden Sie unter SD-WAN Edges.

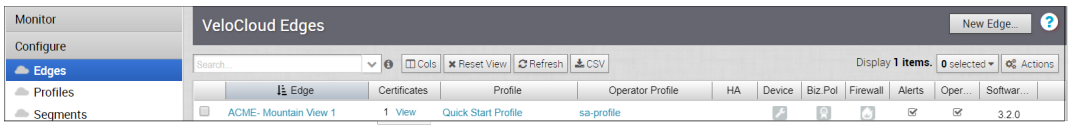
Fehlerbehebung bei Edges

Wenn Sie bei Version 3.4 das Edge 510-LTE-Gerät konfigurieren, können Sie den Diagnosetest „LTE-Modeminformationen“ (LTE Modem Information) ausführen. Während des Diagnosetests **LTE-Modeminformationen (LTE Modem Information)** werden Diagnoseinformationen abgerufen, wie z. B. Signalstärke, Verbindungsinformationen usw. Informationen zum Ausführen eines Diagnosetests finden Sie im Abschnitt Remote-Diagnose.

SD-WAN Edges

Im Konfigurationsbildschirm des SD-WAN Edges sind alle bereitgestellten Edges in einem Unternehmensnetzwerk aufgelistet. Außerdem können Sie hier einen neuen Edge bereitstellen, indem Sie auf die Schaltfläche **Neuer Edge (New Edge)** oben rechts im Bildschirm klicken. Sie können hier auch einen Edge auswählen und verschiedene Aktionen wie z. B. Ändern lokaler Anmeldeinformationen, Löschen eines Edge, Zuweisen eines Profils, Zuweisen eines Operator-Profils und Aktivieren der Vorabbenachrichtigung über das Menü **Aktionen (Actions)** durchführen.

Die nachstehende Tabelle zur *Identifizierung von Enterprise-Edges* enthält Details für jedes Feld und jede Schaltfläche dieses Bildschirms.



Hinweis Wenn Sie mit einer Benutzer-ID angemeldet sind, die über Kundensupport-Berechtigungen verfügt, können Sie nur SD-WAN Orchestrator-Objekte anzeigen. Sie werden nicht in der Lage sein, neue Objekte zu erstellen oder bestehende zu konfigurieren/aktualisieren.

Tabelle zur Identifizierung von Enterprise-Edges

Die meisten Spaltenüberschriften verfügen über eine Sortierfunktion, mit der Elemente in der Spalte in alphabetischer Reihenfolge, numerischer Reihenfolge oder nach Typ aufgelistet werden. (Die Spalten „Gerät“ (Device), „Unternehmensrichtlinie“ (Biz Policy), „Firewall“, „Warnungen“ (Alerts) und „Operator-Warnungen“ (Operator Alerts) haben diese Funktion nicht). Klicken Sie auf die Spaltenüberschriften, die diese Funktion aufweisen, um die Liste zu sortieren.

Option	Beschreibung
Edge	Zeigt den Namen des Edge an. Klicken Sie auf die Spaltenüberschrift **Edge**, um die Edge-Liste in alphabetischer Reihenfolge zu sortieren. Der Edge-Name ist zugleich ein Link. Klicken Sie auf den Link, um den Bildschirm Kapitel 15 Registerkarte „Edge-Übersicht (Edge Overview)“ zu öffnen. Aktivieren Sie das Kontrollkästchen neben dem Namen des Edge, um den Edge auszuwählen.
Zertifikate (Certificates)	Zeigt die aktuellen und abgelaufenen Zertifikate eines Edge an. Klicken Sie auf **Link anzeigen (View link)** neben der Anzahl der Zertifikate, um weitere Informationen zu erhalten.
Profil (Profile)	Listet das Profil auf, das dem Edge zugewiesen ist. Der Profilname ist zugleich ein Link. Wenn Sie auf den Link klicken, wird die Registerkarte Bildschirm „Profilübersicht“ (Profile Overview) geöffnet. HINWEIS: Wenn aufgrund der *Aktivierung per Push* ein Edge-Staging-Profil angezeigt wird, wird dieses Profil von einem neu zugewiesenen Edge verwendet, ist jedoch nicht mit einem Produktionsprofil konfiguriert worden. Enterprise-Administratoren müssen diesen Edges manuell ein Profil zuweisen. Im Abschnitt *Zuweisen eines Profils (Ändern eines Profils)* finden Sie Anweisungen dazu, wie Sie ein Profil manuell einem Edge zuweisen.
Operator-Profil (Operator Profile)	Diese Spalte ist nur für Operatoren sichtbar. Das Operator-Profil ist die Vorlage, die dem Kunden zugewiesen wird, sobald der Kunde von den Operatoren erstellt wird. Dies umfasst das Software-Image, die Anwendungszuordnungen, die Gateway-Auswahl und die Verwaltungseinstellungen des Edge. Administratoren auf Operator-Ebene können das Operator-Profil für bestimmte Edges ändern. Enterprise-Administratoren haben Lesezugriff. Der Name des Operator-Profils ist zugleich ein Link. Wenn Sie auf den Link klicken, wird der Bildschirm *Operator-Profile (Operator Profiles)* geöffnet.
HA	Wenn Sie das Kontrollkästchen **HA** aktivieren, wird die Option „Aktiv/Standby-HA“ (Active Standby HA) aktiviert.
Gerät (Device)	Zeigt ein blaues Symbol ( ) an, wenn Edge-spezifische Konfigurationen vorgenommen wurden. Zeigt ein graues Symbol ( ) an, um anzugeben, dass alle Einstellungen (sofern vorhanden) aus dem Profil übernommen wurden. Um zum Einstellungsbildschirm **Gerät (Device)** zu navigieren, klicken Sie auf das Symbol in der Spalte **Gerät (Device)** und anschließend auf die Registerkarte **Gerät (Device)**.

Option	Beschreibung
Unternehmensrichtlinie (Biz Policy)	Zeigt ein blaues Symbol ( ) an, wenn Regeln für die Unternehmensrichtlinie konfiguriert wurden. Zeigt ein graues Symbol ( ) an, um anzugeben, dass alle Regeln (sofern vorhanden) aus dem Profil übernommen wurden. Um zum Bildschirm **Unternehmensrichtlinie (Business Policy)** zu navigieren, klicken Sie auf das Symbol in der Spalte **Unternehmensrichtlinie (Biz Policy)** und anschließend auf die Registerkarte **Unternehmensrichtlinie (Business Policy)**.
Firewall	Zeigt ein blaues Symbol ( ) an, wenn Firewallregeln konfiguriert wurden. Zeigt ein graues Symbol ( ) an, um anzugeben, dass alle Regeln (sofern vorhanden) aus dem Profil übernommen wurden. Zeigt eine rote Linie quer durch das Symbol ( ) an, wenn die Firewall deaktiviert ist. Wenn die Firewall deaktiviert ist, weist dies darauf hin, dass sie in der Profilkonfiguration eines Edge ausgeschaltet wurde. Um die Firewall zu aktivieren, navigieren Sie zur Profilkonfiguration (Registerkarte **Konfigurieren > Profile > Firewall (Configure > Profiles > Firewall)**). Um zum Bildschirm **Firewall** zu navigieren, klicken Sie auf das Symbol in der Spalte **Firewall** und anschließend auf die Registerkarte **Firewall**.
Warnungen (Alerts)	Wenn Kundenwarnungen für den Edge aktiviert sind, wird das Kontrollkästchen **Warnungen (Alerts)** in dieser Spalte aktiviert. Klicken Sie auf den Namen des Edge in der Spalte **Edge**, um die Kapitel 15 Registerkarte „Edge-Übersicht (Edge Overview)“ zu öffnen und Kundenwarnungen zu aktivieren oder zu deaktivieren.
Operator-Warnungen (Operator Alerts)	Wenn Operator-Warnungen für den Edge aktiviert sind, wird das Kontrollkästchen **Operator-Warnungen (Operator Alerts)** in dieser Spalte aktiviert. Klicken Sie auf den Namen des Edge in der Spalte **Edge**, um die Kapitel 15 Registerkarte „Edge-Übersicht (Edge Overview)“ zu öffnen und Operator-Warnungen zu aktivieren oder zu deaktivieren.
Softwareversion (Software Version)	Die Softwareversion des Edge wird in dieser Spalte angezeigt.
Version der Werkssoftware (Factory Software Version)	Bei der Auslieferung ab Werk ist auf dem Edge eine Standardsoftwareversion enthalten.
Build-Nummer (Build Number)	Zeigt die Build-Nummer eines aktivierten Edge an.
Modell (Model)	Zeigt den Modelltyp des Edge an.
Seriennummer (Serial Number)	Zeigt die Seriennummer des Edge an. Das Zuweisen einer Seriennummer zu einem Edge ist optional. Wenn dem Edge keine Seriennummer zugewiesen ist, ist dieses Feld leer.
Erstellt (Created)	Zeigt das Datum und die Uhrzeit der Bereitstellung des Edge an.
Aktiviert (Activated)	Zeigt das Datum und die Uhrzeit der Edge-Aktivierung an.
Letzter Kontakt (Last Contact)	Das Datum und die Uhrzeit der letzten Kommunikation des Edge mit dem SD-WAN Orchestrator.
Spalte (Column (Cols))	Klicken Sie auf die Schaltfläche **Spalte (Cols)**, um die Optionen auszuwählen, die in der Liste der Enterprise-Edges angezeigt werden sollen (siehe obige Abbildung).
Ansicht zurücksetzen (Reset View)	Setzt die Liste der Enterprise-Edges auf die Standardansicht zurück. (Hiermit werden Filter entfernt und Optionen auf die Standardansicht zurückgesetzt, die aus dem Dropdown-Menü der Schaltfläche **Spalte (Cols)** ausgewählt wurden.)
Aktualisieren (Refresh)	Aktualisiert die Liste der Enterprise-Edges mit aktuellen Daten vom Server.
CSV	Um den in der Liste der Enterprise-Edges angezeigten Inhalt zu exportieren, klicken Sie auf die Schaltfläche **CSV**.

Option	Beschreibung
Ausgewählt (Selected)	Gibt an, wie viele Edges in der Spalte **Edge** ausgewählt werden. Klicken Sie auf die Schaltfläche **Ausgewählt (Selected)**, um alle in der Spalte **Edge** aufgelisteten Edges auszuwählen oder ihre Auswahl aufzuheben.
Aktionen (Actions)	Listet die folgenden Aktionen auf, die Sie für einen ausgewählten Edge durchführen können: ■ **Neuer Edge (New Edge)** ■ **Lokale Anmeldedaten (Local Credentials)** ■ **Edge löschen (Delete Edge)** ■ **Profil zuweisen (Assign Profile)** ■ **Operator-Profil zuweisen (Assign Operator Profile)** ■ **Vorabbenachrichtigungen aktualisieren (Update Pre-notifications)** ■ **Edge-Lizenzierung (Edge Licensing)** ■ **Kundenwarnungen aktualisieren (Update Customer Alerts)** ■ **Gateways neu ausgleichen (Rebalance Gateways)** **Hinweis** „Operator-Profil zuweisen“ (Assign Operator Profile) und „Gateways neu ausgleichen“ (Rebalance Gateways) sind Funktionen auf Operator-Ebene. Weitere Informationen finden Sie unter Bereitstellen eines neuen Edge.
Neuer Edge (New Edge)	Öffnet das Dialogfeld **Neuen Edge bereitstellen (Provision New Edge)**, um einen neuen Edge bereitzustellen. Weitere Informationen finden Sie unter Bereitstellen eines neuen Edge.
Hilfe (Help)	Sie können auf die Online-Hilfe für diese Funktion zugreifen, indem Sie auf das **Fragezeichen** klicken.

Registerkarte „Edge-Übersicht (Edge Overview)“

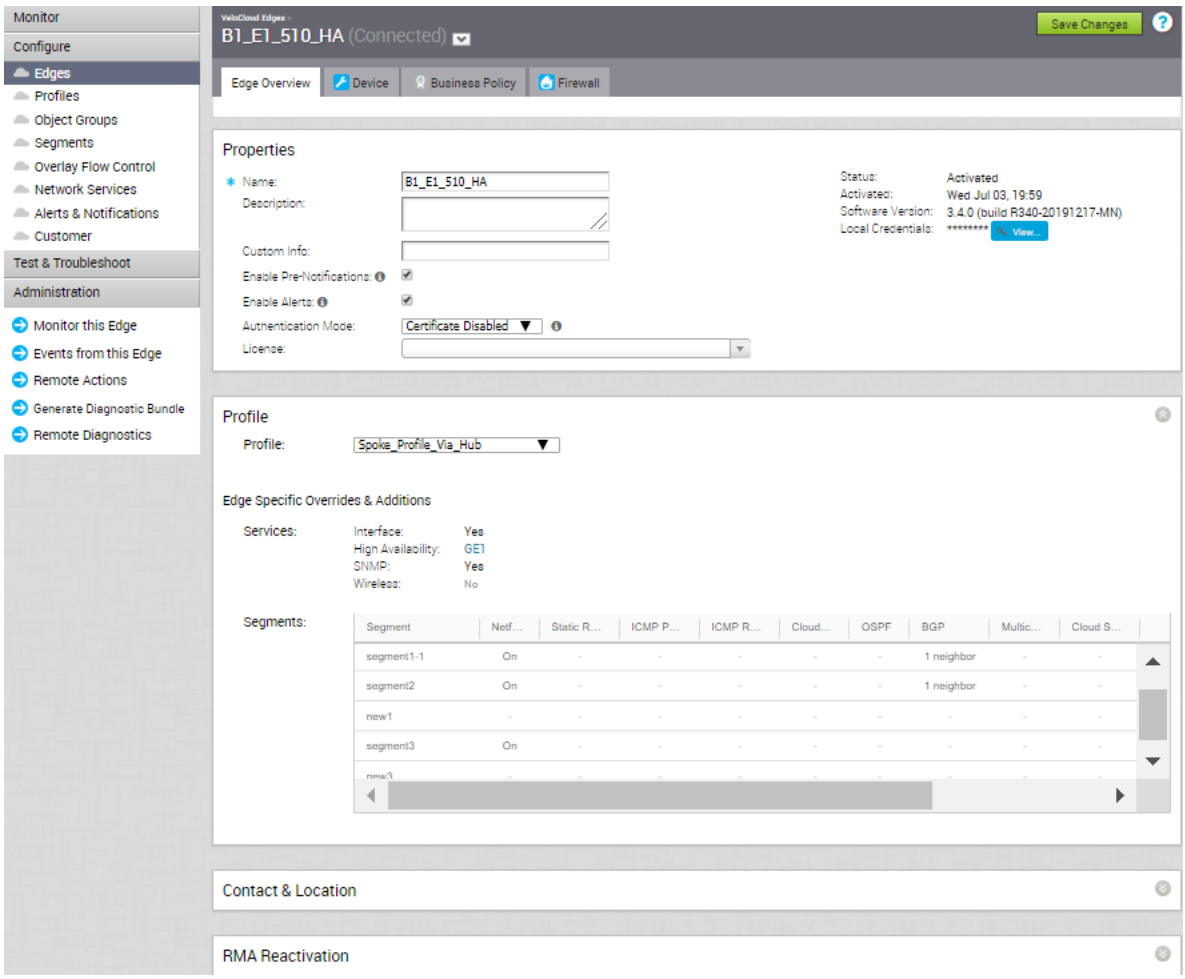
15

Auf der Registerkarte **Edge-Übersicht (Edge Overview)** werden Edge-spezifische Eigenschaftsinformationen bereitgestellt, wie z. B. Name, Beschreibung, benutzerdefinierte Informationen, mit dem Edge verknüpftes Profil, Name und E-Mail-Adresse des Site-Kontakts für den Edge. Über die Registerkarte **Edge-Übersicht (Edge Overview)** können Sie eine Edge-Aktivierungs-E-Mail senden, Warnungen für einen bestimmten Edge aktivieren, Änderungen an bestimmten Eigenschaften vornehmen, ein anderes Profil zu einem ausgewählten Edge hinzufügen, den Edge-Speicherort festlegen, Kontakt- und Standortinformationen des Edge aktualisieren und RMA-Reaktivierung anfordern.

So greifen Sie auf die Registerkarte **Edge-Übersicht (Edge Overview)** zu:

1 Wechseln Sie im Navigationsfenster von SD-WAN Orchestrator zu **Konfigurieren (Configure) > Edges**.

2 Wählen Sie im Bildschirm **Enterprise-Edge (Enterprise Edge)** einen Edge aus und klicken Sie darauf, um die Registerkarte **Edge-Übersicht (Edge Overview)** anzuzeigen.



Auf der Registerkarte **Edge-Übersicht (Edge Overview)**:

- Informationen zum Aktivieren von Warnungen für einen bestimmten Edge oder zum Senden einer Edge-Aktivierungs-E-Mail finden Sie in den Abschnitten *Eigenschaften der Edge-Übersicht* und *Edge-Aktivierung initiieren*.
- Wenn Sie eine Übersicht der Edge-Überschreibungen in einem bestimmten Profil anzeigen möchten oder zu einem anderen Profil wechseln müssen, erhalten Sie weitere Informationen im Abschnitt *Edge-Profil*.
- Informationen zum Ändern des Kontakts, Standorts oder der Versandadresse eines Edge finden Sie im Abschnitt *Edge-Kontakt und -Standort*.
- Informationen zum Anfordern der RMA-Neuaktivierung finden Sie im Abschnitt *RMA-Neuaktivierung*.

Die folgenden Abschnitte enthalten ausführliche Beschreibungen zu allen Bereichen auf der Registerkarte **Edge-Übersicht (Edge Overview)**.

Eigenschaften der Edge-Übersicht

Im Bereich **Eigenschaften (Properties)** können Sie einen Edge-Aktivierungsprozess initiieren, indem Sie eine Edge-Aktivierungs-E-Mail senden. Außerdem können Sie bestimmte Eigenschaften eines ausgewählten Edge anzeigen und ändern. Der Edge-Status, das Aktivierungsdatum und die Softwareversion werden ebenfalls in diesem Bereich angezeigt.

In der folgenden Tabelle werden die Felder im Bereich **Eigenschaften (Properties)** beschrieben.

Feld/Kontrollkästchen	Beschreibung
Name	Zeigt den eindeutigen Namen des Edge auf Kundenebene an. Wenn Sie den Namen des Edge ändern, denken Sie daran, auf die Schaltfläche **Änderungen speichern (Save changes)** zu klicken.
Beschreibung (Description)	Ermöglicht Ihnen, Informationen über den Edge bereitzustellen. Wenn Sie die Beschreibung des Edge aktualisieren, denken Sie daran, auf die Schaltfläche **Änderungen speichern (Save changes)** zu klicken. **Hinweis** Dies ist die einzige Stelle, an der eine Beschreibung des Edge angezeigt wird.
Benutzerdefinierte Info (Custom Info)	Zeigt die benutzerdefinierten Informationen an, die dem Edge zugeordnet sind.
Kontrollkästchen **Vorabbenachrichtigungen aktivieren (Enable Pre-Notifications)**	Dieses Kontrollkästchen ist nach der Bereitstellung des Edge standardmäßig aktiviert. Damit Operatoren Warnungen erhalten, muss das Kontrollkästchen **Vorabbenachrichtigungen aktivieren (Enable Pre-Notifications)** markiert werden. Warnungen müssen über E-Mail, SMS oder SNMP-Traps unter **Konfigurieren (Configure) > Warnungen und Benachrichtigungen (Alerts & Notifications)** ausgewählt und aktiviert werden. Neben dem Empfang von E-Mails, SMS oder SNMP-Traps können Warnungen auch auf dem Bildschirm **Warnungen (Alerts)** unter **Überwachen (Monitor) > Warnungen (Alerts)** angezeigt werden. Deaktivieren Sie dieses Kontrollkästchen, um Warnbenachrichtigungen für Operatoren des ausgewählten Edge zu deaktivieren.
Kontrollkästchen **Warnungen aktivieren (Enable Alerts)**	Dieses Kontrollkästchen ist nach der Bereitstellung des Edge standardmäßig aktiviert. Damit Kunden Warnungen des Edge-Geräts erhalten, muss das Kontrollkästchen **Warnungen aktivieren (Enable Alerts)** aktiviert werden. Warnungen müssen über E-Mail, SMS oder SNMP-Traps unter **Konfigurieren (Configure) > Warnungen und Benachrichtigungen (Alerts & Notifications)** ausgewählt und aktiviert werden. Neben dem Empfang von E-Mails, SMS oder SNMP-Traps können Warnungen auch auf dem Bildschirm **Warnungen (Alerts)** unter **Überwachen (Monitor) > Warnungen (Alerts)** angezeigt werden. Heben Sie die Markierung dieses Kontrollkästchens auf, um Warnungen des ausgewählten Edge zu deaktivieren.

Feld/Kontrollkästchen	Beschreibung
Authentifizierungsmodus (Authentication Mode)	Für den Authentifizierungsmodus stehen drei Optionen zur Verfügung: „Zertifikat deaktiviert (Certificate Disabled)“, „Zertifikat optional (Certificate Optional)“ und „Zertifikat erforderlich (Certificate Required)“. ■ **Zertifikat deaktiviert (Standardeinstellung) (Certificate Disabled):** Bei Auswahl von „Zertifikat deaktiviert (Certificate Disabled)“ verwendet der Edge einen Authentifizierungsmodus vom Typ „Vorinstallierter Schlüssel“. ■ **Zertifikat optional (Certificate Optional):** Bei Auswahl von „Zertifikat optional (Certificate Optional)“ verwendet der Edge entweder das PKI-Zertifikat oder den vorinstallierten Schlüssel (je nach dem Zertifikat, das von dem anderen Edge oder Gateway verwendet wird). **Hinweis** Der Operator muss PKI unter „Konfigurieren > Kunde (Configure > Customer)“ aktivieren. ■ **Zertifikat erforderlich (Certificate Required):** Sobald der Edge ein gültiges Zertifikat erhält, steht „Zertifikat erforderlich (Certificate Required)“ als Option im Dropdown-Menü zur Verfügung. Wenn die Option „Zertifikat erforderlich (Certificate required)“ ausgewählt ist, verwendet der Edge das PKI-Zertifikat als Authentifizierungsmodus. **Hinweis** Der Operator muss PKI unter **Konfigurieren > Kunde (Configure > Customer)** aktivieren.
Lizenz (License)	Im Dropdown-Menü **Lizenz (License)** werden verfügbare Lizenztypen angezeigt, die einem Edge zugewiesen werden können. **Hinweis** Standardadministrator-Superuser und Standardadministratoren können Edge-Lizenztypen zuweisen und überwachen, die ihnen zugeteilt wurden.
Zertifikat anzeigen (View Certificate)	Wenn der Edge über ein gültiges Zertifikat verfügt, wird der Link **Anzeigen (View)** angezeigt. Klicken Sie auf den Link **Anzeigen (View)**, um das Zertifikat anzuzeigen, zu exportieren oder zu widerrufen.
Status	Zeigt die folgenden Statusoptionen an: Ausstehend (Pending), Aktiviert (Activated) und Neuaktivierung ausstehend (Reactivation Pending). ■ **Ausstehend (Pending):** Der Edge wurde nicht aktiviert. ■ **Aktiviert (Activated):** Der Edge wurde aktiviert. ■ **Neuaktivierung ausstehend (Reactivation Pending):** Wenn Sie auf die Schaltfläche **Neuaktivierung anfordern (Request Reactivation)** klicken, wird der Status in „Neuaktivierung ausstehend (Reactivation Pending)“ geändert. Mit dieser Statusaktualisierung wird die Funktion des Edge nicht geändert. Es wird lediglich angegeben, dass ein neuer oder Ersatz-Edge mit der vorhandenen Konfiguration aktiviert werden kann.
Aktiviert (Activated)	Zeigt das Datum und die Uhrzeit der Edge-Aktivierung an.
Softwareversion (Software Version)	Zeigt die Softwareversion und die Build-Nummer des Edge an.
Lokale Anmeldedaten (Local Credentials)	Zeigt die Anmeldedaten für die lokale Benutzeroberfläche an. Die Standardanmeldedaten lauten Benutzername: Administratorkennwort: admin123 (Groß-/Kleinschreibung muss beachtet werden). Klicken Sie auf die Schaltfläche **Anzeigen (View)**, um die Anmeldedaten zu ändern.

Feld/Kontrollkästchen	Beschreibung
Seriennummer (Serial Number)	Wenn der Edge den Status „Ausstehend (Pending)“ aufweist, wird das Textfeld **Seriennummer (Serial Number)** angezeigt. Die Eingabe der Seriennummer ist optional. Wenn sie jedoch angegeben wird, muss die Seriennummer mit der Seriennummer des Edge übereinstimmen, der aktiviert wird.
Aktivierungsschlüssel (Activation Key)	Wenn der Edge den Status „Ausstehend (Pending)“ aufweist, wird der Edge-Aktivierungsschlüssel angezeigt. Der Aktivierungsschlüssel ist nur einen Monat gültig. Nach einem Monat läuft der Schlüssel ab, und eine Warnmeldung wird unterhalb des Aktivierungsschlüssels angezeigt. Sie können einen neuen Schlüssel erzeugen, indem Sie auf die Schaltfläche **Neuen Aktivierungsschlüssel generieren (Generate New Activation Key)** unter der Warnmeldung klicken. Weitere Informationen finden Sie im Abschnitt *Abgelaufener RMA-Aktivierungsschlüssel*.
Aktivierungs-E-Mail senden (Send Activation Email)	Wenn Sie auf **Aktivierungs-E-Mail senden (Send Activation Email)** klicken, wird eine E-Mail mit Aktivierungsanweisungen an den Site-Kontakt gesendet.

Initiieren der Edge-Aktivierung

Nach dem Speichern der Edge-Konfiguration wird ein Aktivierungsschlüssel zugewiesen. Klicken Sie im Bereich **Eigenschaften (Properties)** auf die Schaltfläche **Aktivierungs-E-Mail senden (Send Activation Email)**, um die Edge-Aktivierung zu initiieren. Durch Klicken auf **Aktivierungs-E-Mail senden (Send Activation Email)** wird der Edge nicht aktiviert. Lediglich der Aktivierungsvorgang wird initiiert, indem eine E-Mail mit Anweisungen zum Aktivieren des Edge-Geräts an den Site-Kontakt gesendet wird.

Nach dem Klicken auf die Schaltfläche **Aktivierungs-E-Mail senden (Send Activation Email)** wird ein Popup-Fenster mit der E-Mail angezeigt, die an den Site-Kontakt gesendet wird. Anweisungen zum Verbinden und Aktivieren der Edge-Hardware werden in der E-Mail an den Site-Kontakt bereitgestellt. Weitere Informationen zum Aktivieren eines Edge finden Sie in der *Kurzanleitung zur Edge-Aktivierung* in der Online-Hilfe. Informationen zur Pull- und Push-Aktivierung finden Sie unter *Zero Touch-Bereitstellung*.

Edge-Profil

Im Dropdown-Menü **Profil (Profile)** wird eine Liste der Profile angezeigt, die einem bestimmten Edge zugewiesen werden können. Wenn Sie zu einem anderen Profil auf dem Edge wechseln, werden alle relevanten Konfigurationen mit Ausnahme der Edge-Überschreibungskonfigurationen geändert. Überschriebene Konfigurationen werden im Bereich **Profil (Profile)** angezeigt.

Hinweis Vom Edge überschriebene Konfigurationen werden beim Wechsel zu einem anderen Profil nicht geändert.

Hinweis Wenn ein Edge-Staging-Profil aufgrund von Push-Aktivierung als Option angezeigt wird, handelt es sich um einen neu zugewiesenen Edge, der nicht von einem Produktionsprofil konfiguriert wurde. Enterprise-Administratoren müssen diesen Edges manuell ein Profil zuweisen, indem sie ein neues Profil im Dropdown-Menü **Profil (Profile)** auswählen.

Auswahl des Operator-Profils

In der folgenden Tabelle wird eine Kompatibilitätsmatrix für ein vom Kunden zugewiesenes Operator-Profil sowie für ein vom Edge zugewiesenes Enterprise-Profil bereitgestellt: Beim Wechseln von Profilen finden Sie Informationen in dieser Matrix.

Matrix zur Auswahl des Operator-Profils (Operator Profile Selection Matrix)

Profiltyp des Kunden-Operators	Aktuelles Edge-Enterprise-Profil	Ausgewähltes Edge-Enterprise-Profil	Ergebnis
Segmentbasiert	Segmentbasiert	Segmentbasiert	Keine Änderung
Netzwerkbasiert	Netzwerkbasiert	Netzwerkbasiert	Keine Änderung
Segmentbasiert	Netzwerkbasiert	Segmentbasiert	Die Edge-Konfiguration wird in eine segmentbasierte Konfiguration umgewandelt. Diese wird dem Edge jedoch erst bereitgestellt, wenn das Edge-Software-Image auf eine Version ≧ 3.0 aktualisiert wird.
Netzwerkbasiert	Netzwerkbasiert	Segmentbasiert	Die Edge-Konfiguration wird in eine segmentbasierte Konfiguration umgewandelt. Diese wird dem Edge jedoch erst bereitgestellt, wenn das Edge-Software-Image auf eine Version ≧ 3.0 aktualisiert wird.
Segmentbasiert	Netzwerkbasiert	Netzwerkbasiert	Der Edge empfängt das Image-Update nicht.
Netzwerkbasiert	Segmentbasiert	Segmentbasiert	Der Edge empfängt das Image-Update nicht.

Bei den Edge-Überschreibungen handelt es sich um Änderungen an den vererbten Profilkonfigurationen auf Edge-Ebene. Edge-Erweiterungen sind Konfigurationen, die nicht im Profil enthalten sind, dem ausgewählten Edge aber hinzugefügt werden. Eine Übersicht über alle Edge-Überschreibungen und -Erweiterungen werden im Profilbereich angezeigt

Edge-Kontakt und -Standort

Im Bereich **Kontakt und Standort (Contact & Location)** werden die Edge-Kontaktinformationen und der Edge-Standort angezeigt. Hier können Sie auch den Standort und die Versandadresse des Edge ändern.

So ändern Sie die Adresse des Edge:

1 Klicken Sie auf den Link **Standort aktualisieren (Update Location)**.

2 Aktualisieren Sie den Standort im Popup-Fenster **Edge-Standort einrichten (Set Edge Location)**, indem Sie entweder die Funktion **Adresse suchen (Search Address)** (standardmäßig ausgewählt) verwenden oder die Adresse manuell eingeben.

3 Zur manuellen Eingabe klicken Sie auf die Schaltfläche **Manueller Adresseintrag (Manual Address Entry)** und geben entweder die Adresse oder den Längen- und Breitengrad ein.

4 Wenn Sie die Adresse eingeben möchten, klicken Sie auf die Schaltfläche **Längen- und Breitengrad aus Adresse aktualisieren (Update Lat,Lng From Address)**.

5 Wenn Sie den Längen- und Breitengrad eingeben möchten, klicken Sie auf die Schaltfläche **Adresse aus Längen- und Breitengrad aktualisieren (Update Address From Lat,Lng)**.

6 Klicken Sie nach Abschluss des Vorgangs auf **OK**.

Wenn sich die Versandadresse vom Standort des Edge unterscheidet, deaktivieren Sie das Kontrollkästchen **Wie oben (Same as above)** für die Versandadresse und geben Sie dann im entsprechenden Textfeld den Versandkontakt ein.

So ändern Sie den Versandort des Edge:

1 Klicken Sie auf den Link **Standort festlegen (Set Location)**.

2 Aktualisieren Sie den Versandort im Popup-Fenster **Versandort des Edge (Edge Shipping Location)**, indem Sie entweder die Funktion **Adresse suchen (Search Address)** (standardmäßig ausgewählt) verwenden oder die Adresse manuell eingeben.

3 Zur manuellen Eingabe der Adresse klicken Sie auf die Schaltfläche **Manueller Adresseintrag (Manual Address Entry)**, geben die Adresse ein und klicken dann auf die Schaltfläche **Standort auf Karte aktualisieren (Update Location on Map)**.

4 Klicken Sie auf **OK**.

RMA-Neuaktivierung

In folgenden Szenarien können Sie eine Edge-Anfrage zur RMA-Neuaktivierung über die Registerkarte **Edge-Übersicht (Edge Overview)** initiieren:

- Ersetzen eines Edge aufgrund eines Fehlers
- Aktualisieren eines Edge-Hardwaremodells

So schließen Sie den RMA-Neuaktivierungsprozess ab:

1 Navigieren Sie im Orchestrator zu **Konfigurieren (Configure) > Edges**.

2 Wählen Sie den Edge aus, die erneut aktiviert werden soll.

3 Führen Sie auf der Registerkarte **Edge-Übersicht (Edge Overview)** einen Bildlauf nach unten zum Bereich **RMA-Neuaktivierung (RMA Reactivation)** durch. Erweitern Sie den Bereich, indem Sie oben rechts auf den grauen Pfeil klicken.

4 Klicken Sie auf die Schaltfläche **Neuaktivierung anfordern (Request Reactivation)**. In diesem Schritt wird ein neuer Aktivierungsschlüssel erstellt, und der Edge-Status wird in den Modus „Neuaktivierung ausstehend (Reactivation Pending)“ versetzt.

Hinweis Der Neuaktivierungsschlüssel ist nur einen Monat ab dem Zeitpunkt der Neuaktivierungsanforderung gültig.

5 Wenn Sie die Aktivierungsanforderung aus einem beliebigen Grund abbrechen müssen, klicken Sie auf die Schaltfläche **Neuaktivierungsanforderung abbrechen (Cancel Reactivation Request)**. Der Edge-Status wechselt von **Neuaktivierung ausstehend (Reactivation Pending)** zu **Aktiviert (Activated)**.

6 Nach Ablauf des Aktivierungsschlüssels (der Schlüssel ist einen Monat gültig) müssen Sie einen neuen Aktivierungsschlüssel generieren. Weitere Informationen finden Sie im Abschnitt *Abgelaufener RMA-Aktivierungsschlüssel (Expired RMA Activation Key)*.

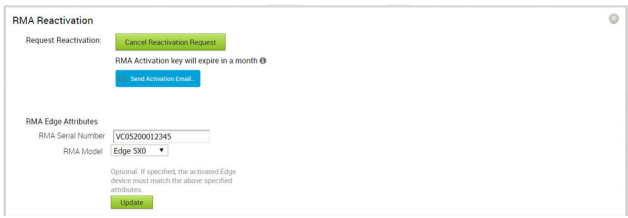
7 Als optionalen Schritt können Sie die Seriennummer des Edge eingeben, der im Textfeld „RMA-Seriennummer (RMA Serial Number)“ aktiviert wird.

Hinweis Seriennummern unterliegen der Groß-/Kleinschreibung. Die Aktivierung schlägt fehl, wenn die Seriennummer nicht mit dem zu aktivierenden Edge übereinstimmt.

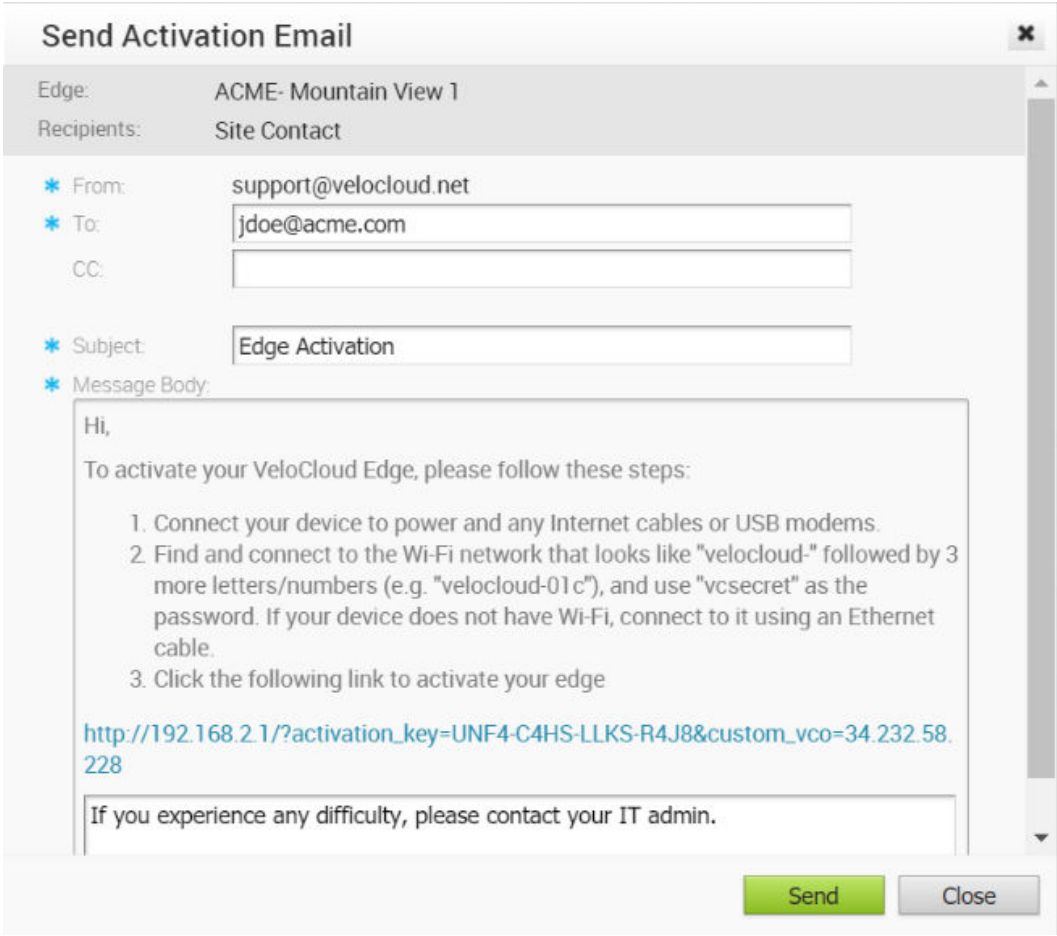
8 Der ausgewählte Edge wird standardmäßig im Dropdown-Menü **RMA-Modell (RMA Model)** angezeigt. Wenn Sie ein anderes Edge-Modell erneut aktivieren, wählen Sie das zu aktivierende Edge-Modell im Dropdown-Menü **RMA-Modell (RMA Model)** aus.

Hinweis Die Aktivierung schlägt fehl, wenn das ausgewählte Edge-Modell nicht mit dem zu aktivierenden Edge übereinstimmt.

9 Wenn Sie eine Seriennummer eingegeben oder ein Modell im Dropdown-Menü „RMA-Modell (RMA Model)“ ausgewählt haben, klicken Sie auf die Schaltfläche **Aktualisieren (Update)**.



10 Klicken Sie auf die Schaltfläche **Aktivierungs-E-Mail senden (Send Activation Email)**. Das Popup-Fenster **Aktivierungs-E-Mail senden (Send Activation Email)** wird angezeigt.



11 Klicken Sie auf die Schaltfläche **Senden (Send)**, um die Aktivierungs-E-Mail an den Site-Kontakt zu senden. Diese E-Mail enthält dieselben Informationen, die auch im Popup-Fenster **Aktivierungs-E-Mail senden (Send Activation Email)** angezeigt werden.

Die übrigen Anweisungen enthalten Schritte zum Aktivieren des Edge-Ersatzgeräts.

12 Trennen Sie den alten Edge von der Stromversorgung und vom Netzwerk.

13 Verbinden Sie den neuen Edge mit der Stromversorgung und dem Netzwerk. Stellen Sie sicher, dass der Edge mit dem Internet verbunden ist.

14 Verwenden Sie das Aktivierungsverfahren, das Sie per E-Mail erhalten haben.

Hinweis Klicken Sie auf den Aktivierungslink in der E-Mail, um den Edge zu aktivieren.

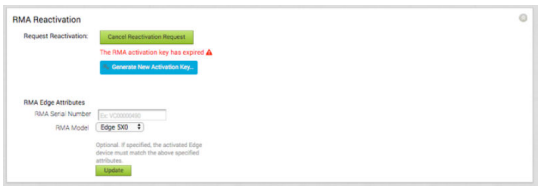
Der Edge lädt die Konfiguration und Software aus dem SD-WAN Orchestrator herunter. Der neue Edge wird erfolgreich aktiviert und ist dienstbereit.

Abgelaufener RMA-Aktivierungsschlüssel

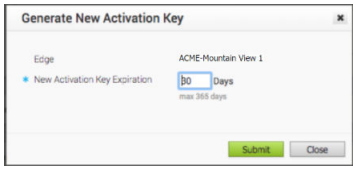
Der RMA-Aktivierungsschlüssel ist einen Monat ab dem Zeitpunkt der Neuaktivierungsanforderung gültig. Nach Ablauf des RMA-Aktivierungsschlüssels wird eine Warnmeldung im Bereich „RMA-Neuaktivierung (RMA Reactivation)“ des SD-WAN Orchestrator angezeigt. Sie können die Neuaktivierungsanforderung entweder abbrechen (indem Sie auf die Schaltfläche **Neuaktivierungsanforderung abbrechen (Cancel Reactivation Request)** klicken) oder einen neuen Schlüssel generieren. Befolgen Sie die folgenden Anweisungen, um nach Ablauf des Aktivierungsschlüssels einen neuen Schlüssel zu generieren.

So generieren Sie einen neuen RMA-Aktivierungsschlüssel:

1 Klicken Sie auf die Schaltfläche **Neuen Aktivierungsschlüssel generieren (Generate New Activation Key)**.



2 Geben Sie im Dialogfeld **Neuen Aktivierungsschlüssel generieren (Generate New Activation Key)** die Anzahl der Tage ein, die der Schlüssel aktiv sein soll.



3 Klicken Sie auf **Übermitteln (Submit)**.

4 Führen Sie die *Schritte zur RMA-Neuaktivierung* durch, um den RMA-Neuaktivierungsprozess abzuschließen.

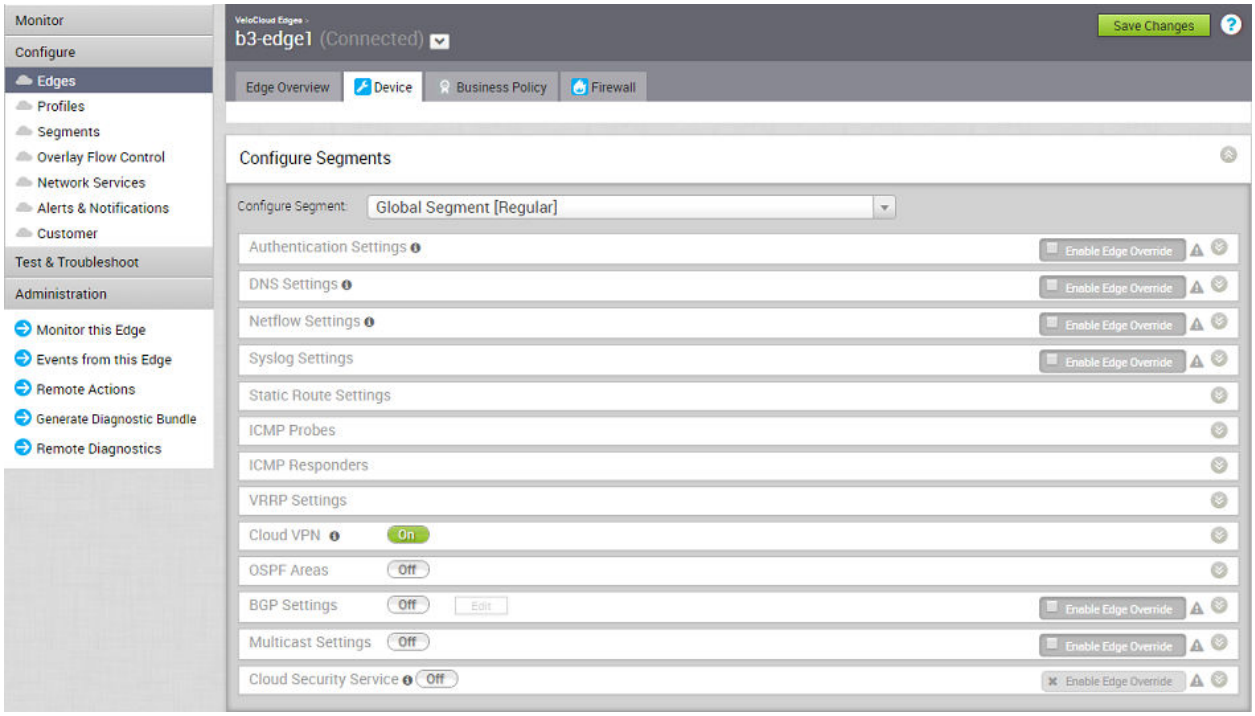
Konfigurieren eines Edge-Geräts 16

Einige Einstellungen, die einem Edge zugewiesen wurden, können durch die Konfiguration außer Kraft gesetzt werden. In den meisten Fällen muss eine Außerkraftsetzung zuerst aktiviert werden, dann können Änderungen vorgenommen werden.

Außerkraftsetzungen können an Schnittstellen, DNS und Authentifizierung vorgenommen werden. Darüber hinaus können Außerkraftsetzungsregeln zu bestehenden Unternehmensrichtlinien und Firewall-Regeln hinzugefügt werden. Außerkraftsetzungsregeln haben Vorrang vor allen anderen Regeln, die für die Unternehmensrichtlinie oder Firewall definiert sind.

Hinweis Edge-Außerkraftsetzungen ermöglichen Edge-spezifische Bearbeitungen der angezeigten Einstellungen und unterbinden weitere automatische Aktualisierungen aus dem Konfigurationsprofil. Sie können die Außerkraftsetzung einfach deaktivieren und jederzeit zu automatischen Updates zurückkehren.

In den folgenden Abschnitten werden die Bereiche auf der Registerkarte **Konfigurieren > Edges > Gerät (Configure > Edges > Device)** beschrieben.



Einige Bereiche sind segmentierfähig.

Segmentierfähige Konfigurationen

- Authentifizierungseinstellungen
- DNS-Einstellungen
- NetFlow-Einstellungen
- Syslog-Einstellungen
- Einstellungen für statische Route
- ICMP-Tests
- ICMP-Responder
- VRRP-Einstellungen
- Cloud-VPN
- OSPF-Bereiche
- BGP-Einstellungen
- Multicast-Einstellungen
- Cloud-Sicherheitsdienst

Häufige Konfigurationen:

- Hochverfügbarkeit
- VLAN
- Geräteeinstellungen
- WAN-Einstellungen
- QoS mit Mehrfachquelle
- SNMP-Einstellungen
- NTP-Server
- Sichtbarkeitsmodus

Hinweis Weitere Informationen zu OSPF und BGP finden Sie im Abschnitt Kapitel 19 Konfigurieren von dynamischem Routing mit OSPF oder BGP.

Dieses Kapitel enthält die folgenden Themen:

- Konfigurieren von DSL-Einstellungen
- Konfigurieren der Netflow-Einstellungen auf der Edge-Ebene
- Konfigurieren von Syslog-Einstellungen auf der Edge-Ebene
- Konfigurieren der Einstellungen für statische Routen
- Konfigurieren von ICMP-Tests/-Respondern
- Konfigurieren von VRRP-Einstellungen
- Edge-Cloud-VPN
- Konfigurieren von VLAN für Edges
- Konfigurieren von Geräteeinstellungen
- Konfigurieren von SNMP-Einstellungen auf der Edge-Ebene
- Konfigurieren von Außerkraftsetzungen für WLAN-Funk
- Sicherheits-VNFs
- Konfigurieren der Edge-Unternehmensrichtlinie
- Konfigurieren der Edge-Aktivierung
- LAN-seitige NAT-Regeln auf Edge-Ebene

Konfigurieren von DSL-Einstellungen

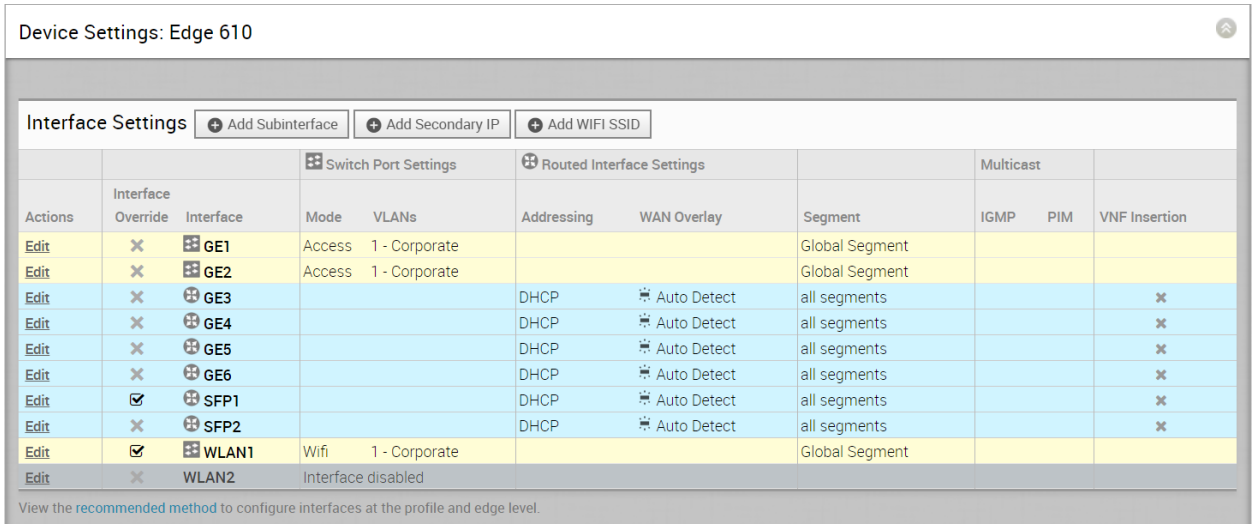
Unterstützung ist für das Metanoia xDSL SFP-Modul (MT 5311) verfügbar. Es handelt sich um ein hochintegriertes SFP-Überbrückungsmodem, das eine austauschbare SFP-kompatible

Schnittstelle bietet, um vorhandene DSL IAD- oder Heim-Gateway-Geräte auf Dienste mit höherer Bandbreite aufzurüsten.

Das Metanoia xDSL-SFP-Modul (MT 5311) kann am SFP-Steckplatz des Edge 610-Geräts angeschlossen und im ADSL2+/VDSL2-Modus verwendet werden. Dieses Modul muss vom Benutzer beschafft werden. Das Konfigurieren von DSL ist nur für das 610 Edge-Gerät verfügbar.

Konfigurieren von SFP

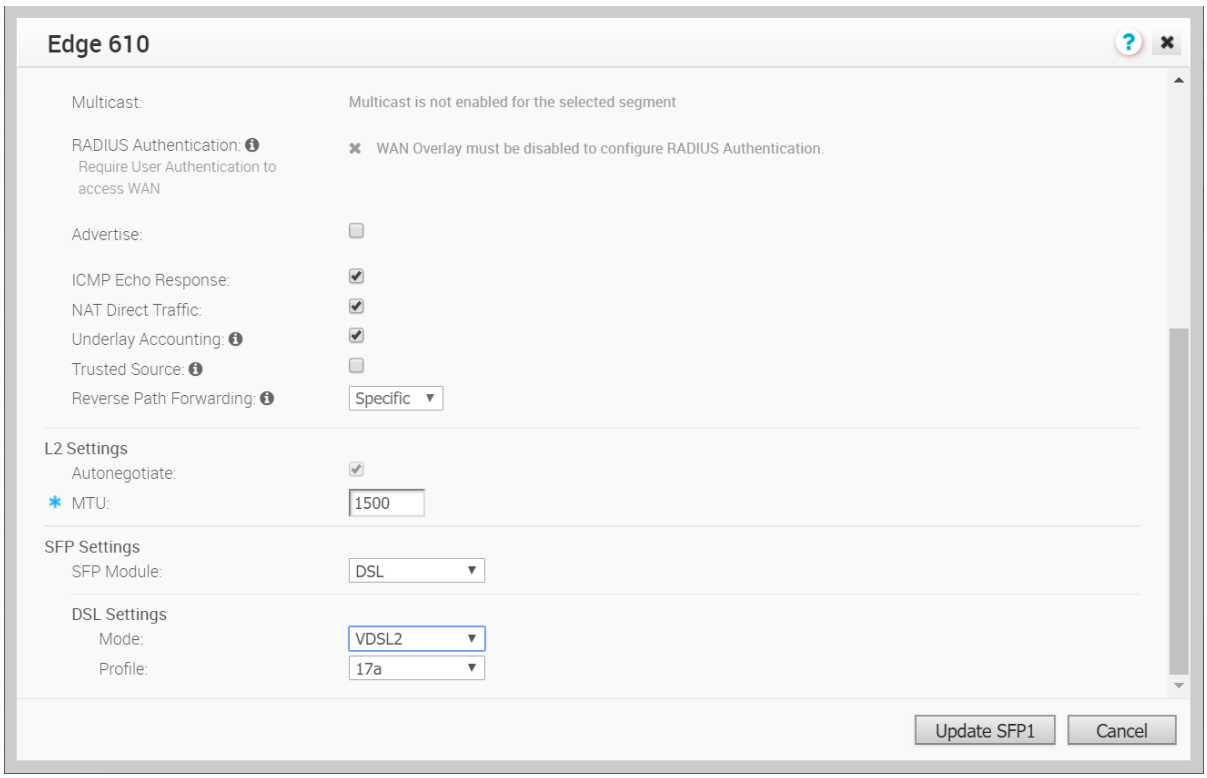
Klicken Sie auf die SFP-Schnittstelle, an die das jeweilige DSL-Modul angeschlossen ist. Wenn das SFP angeschlossen ist, wird der Steckplatzname als SFP1 und SFP2 angezeigt.



So konfigurieren Sie SFP:

1 Klicken Sie auf den Link **Bearbeiten (Edit)** in der Spalte **Aktionen (Actions)**, wie in der obigen Abbildung dargestellt.

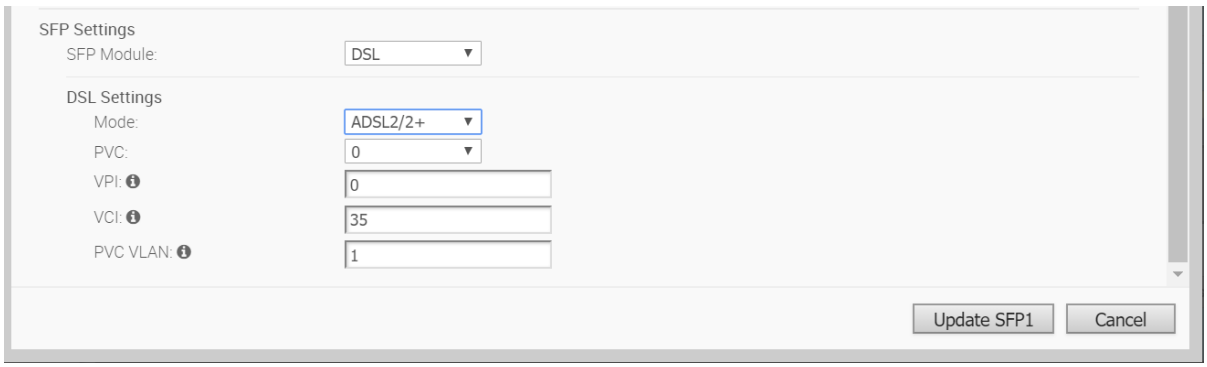
Das Dialogfeld **Schnittstelle SFP1 (Interface SFP1)** wird für das Edge-Gerät (Edge 610 in diesem Beispiel) angezeigt, wie in der Abbildung unten dargestellt.



2 Das Kontrollkästchen **Schnittstelle außer Kraft setzen (Override Interface)** muss aktiviert werden, um die DSL-Einstellungen zu konfigurieren.

3 Aktivieren Sie das Kontrollkästchen **Schnittstelle aktiviert (Interface Enabled)**.

4 Im Bereich **SFP-Einstellungen (SFP Settings)** stehen im Dropdown-Menü zwei Optionen zur Verfügung: „Standard“ und „DSL“. Wählen Sie **DSL** als SFP-Modul aus, wie in der folgenden Abbildung dargestellt.



5 Wählen Sie im Bereich **DSL-Einstellungen (DSL Settings)** den Modus und die Profileinstellungen wie nachfolgend beschrieben aus (in der Tabelle „DSL-Einstellungen (DSL Settings)“ finden Sie eine Beschreibung der verfügbaren Optionen):

   a Wählen Sie im Dropdown-Menü **Modus (Mode)** eine der beiden Optionen aus: **VDSL 2** oder **ADSL2/2+**. Wenn Sie die Option **ADSL2/2+** als Modus wählen, konfigurieren Sie die folgenden Einstellungen.

      1 Wählen Sie im Dropdown-Menü **PVC** eine PVC-Nummer aus (0-7).

      2 Geben Sie eine VPI-Nummer ein oder wählen Sie mit den Auf-/Ab-Pfeilen eine Nummer im Textfeld **VPI** aus.

      3 Geben Sie eine VCI-Nummer ein oder wählen Sie mit den Auf-/Ab-Pfeilen eine Nummer im Textfeld **VCI** aus.

      4 Geben Sie eine PVC VLAN-Nummer ein oder wählen Sie mit den Auf-/Ab-Pfeilen eine Nummer im Textfeld **PVC VLAN** aus.

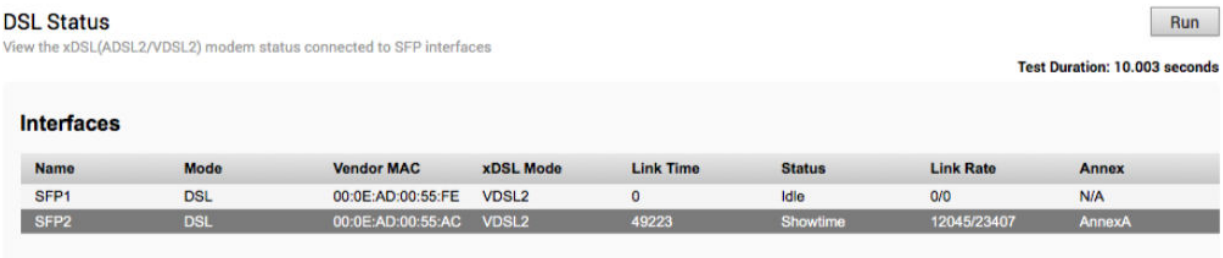
   b Wählen Sie im Dropdown-Menü **Profil (Profile)** entweder „30a“ oder „17a“ aus.

6 DHCP-Servertyp.

7 Klicken Sie auf die **SFP1 aktualisieren (Update SFP1)**.

Fehlerbehebung bei DSL-Einstellungen

DSL-Diagnosetest: (DSL Diagnostic Test:) Der DSL-Diagnosetest ist nur für 610 Geräte verfügbar. Bei der Durchführung dieses Tests wird der DSL-Status angezeigt, der Informationen wie „Modus (Mode)“ (Standard oder DSL), „Profil (Profile)“, „xDSL-Modus (xDSL Mode)“ usw. enthält, wie in der folgenden Abbildung dargestellt.



Konfigurieren der Netflow-Einstellungen auf der Edge-Ebene

Als Unternehmensadministrator können Sie auf der Edge-Ebene die im Profil angegebenen Netflow-Einstellungen überschreiben, indem Sie das Kontrollkästchen **Edge-Außerkraftsetzung aktivieren (Enable Edge Override)** aktivieren.

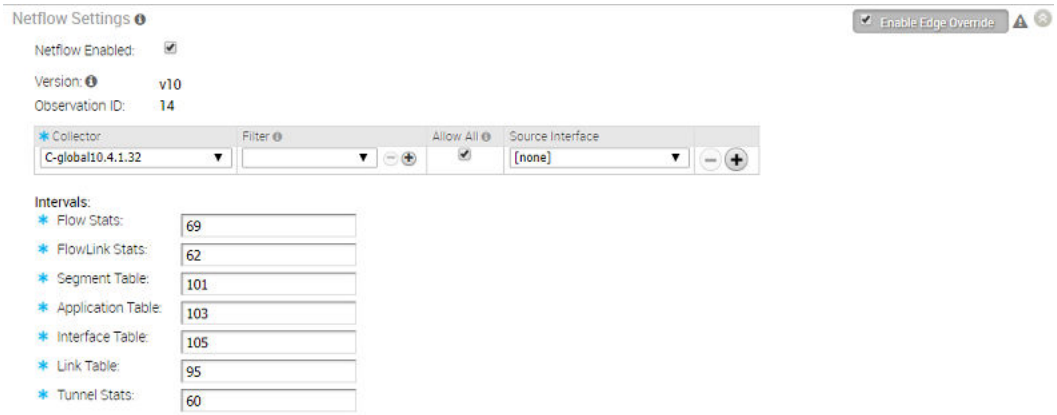
Verfahren

1 Navigieren Sie in der SD-WAN Orchestrator-Instanz zu **Konfigurieren (Configure)** > **Edges**.

Die Seite **VeloCloud Edges** wird angezeigt.

2 Wählen Sie einen Edge aus, für den Sie die NetFlow-Einstellungen überschreiben möchten, und klicken Sie auf das Symbol in der Spalte **Gerät (Device)**.

Die Seite „Geräteeinstellung (Device Setting)“ für den ausgewählten Edge wird angezeigt.



3 Wählen Sie im Dropdown-Menü **Segment konfigurieren (Configure Segment)** ein Profilsegment aus, um die NetFlow-Einstellungen zu konfigurieren.

4 Navigieren Sie zum Bereich **Netflow-Einstellungen (Netflow Settings)** und aktivieren Sie das Kontrollkästchen **Edge-Außerkraftsetzung aktivieren (Enable Edge Override)**.

Auf der Edge-Ebene wird das Feld **Beobachtungs-ID (Observation ID)** automatisch mit einer 8-Bit-Segment-ID und einer 24-Bit-Edge-ID ausgefüllt und kann nicht bearbeitet werden. Die Beobachtungs-ID ist für einen Exportvorgang pro Segment und Unternehmen eindeutig.

5 Überschreiben Sie die im Profil angegebenen Collector-, Filter- und Netflow-Exportintervallinformationen, indem Sie sich auf Schritt 4 in Konfigurieren von Netflow-Einstellungen auf der Profilebene beziehen.

6 Wählen Sie im Dropdown-Menü **Quellschnittstelle (Source Interface)** eine Edge-Schnittstelle aus, die im Segment als Quellschnittstelle konfiguriert ist, und wählen Sie die Quell-IP für die NetFlow-Pakete aus.

Hinweis Achten Sie darauf, die LAN-Schnittstelle von Edge (VLAN/Geroutet/Teilschnittstelle) mit aktiviertem Flag „Ankündigen (Advertise)“ als Quellschnittstelle manuell auszuwählen. Wenn **keine (none)** ausgewählt ist, wählt der Edge aus dem entsprechenden Segment als Quellschnittstelle für jenen Collector automatisch eine LAN-Schnittstelle (VLAN/Geroutet/Teilschnittstelle) aus, die „AKTIV“ ist, und bei der „Ankündigen (Advertise)“ aktiviert ist. Wenn der Edge keine Schnittstellen mit dem Status „AKTIV“ und aktiviertem „Ankündigen (Advertise)“ hat, wird die Quellschnittstelle nicht gewählt und die Netflow-Pakete werden nicht erstellt.

7 Klicken Sie auf **Änderungen speichern (Save Changes)**.

Konfigurieren von Syslog-Einstellungen auf der Edge-Ebene

In einem Unternehmensnetzwerk unterstützt SD-WAN Orchestrator die Erfassung von SD-WAN Orchestrator-gebundenen Ereignissen und Firewallprotokollen, die vom Unternehmens-SD-WAN Edges stammen, in einer oder mehreren zentralen Remote-Syslog-Collector-Instanzen (Server) im nativen Syslog-Format. Auf der Edge-Ebene können Sie die im Profil angegebenen Syslog-Einstellungen außer Kraft setzen, indem Sie das Kontrollkästchen **Edge-Außerkraftsetzung aktivieren (Enable Edge Override)** aktivieren.

Führen Sie die folgenden Schritte aus, um die Syslog-Einstellungen auf der Edge-Ebene außer Kraft zu setzen.

Voraussetzungen

- Stellen Sie sicher, dass Cloud-VPN (Zweigstelle-zu-Zweigstelle-VPN-Einstellungen) für den SD-WAN Edge konfiguriert ist (von dem die SD-WAN Orchestrator-gebundenen Ereignisse stammen), um einen Pfad zwischen dem SD-WAN Edge und den Syslog-Collectors herzustellen. Weitere Informationen finden Sie unter Konfigurieren von Cloud-VPN.

Verfahren

1 Navigieren Sie in der SD-WAN Orchestrator-Instanz zu **Konfigurieren (Configure)** > **Edges**.

Die Seite SD-WAN Edges wird angezeigt.

2 Wählen Sie einen Edge aus, für den Sie die Syslog-Einstellungen außer Kraft setzen möchten, und klicken Sie auf das Symbol in der Spalte **Gerät (Device)**.

Die Seite „Geräteeinstellungen (Device Settings)“ wird für den ausgewählten Edge angezeigt.

3 Wählen Sie im Dropdown-Menü **Segment konfigurieren (Configure Segment)** ein Profilsegment aus, um die Syslog-Einstellungen zu konfigurieren. Standardmäßig ist **Globales Segment [Normal] (Global Segment [Regular])** ausgewählt.

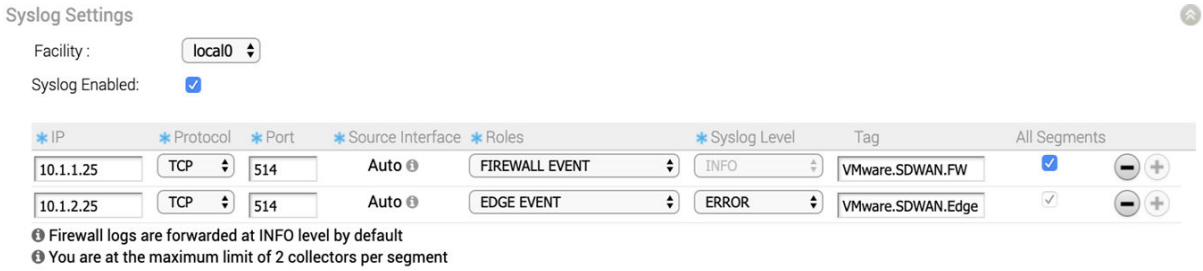
4 Navigieren Sie zum Bereich **Syslog-Einstellungen (Syslog Settings)** und aktivieren Sie das Kontrollkästchen **Edge-Außerkraftsetzung aktivieren (Enable Edge Override)**.

5 Wählen Sie im Dropdown-Menü **Quellschnittstelle (Source Interface)** eine der im Segment konfigurierten Edge-Schnittstellen als Quellschnittstelle aus.

6 Überschreiben Sie die anderen im Profil verknüpften Syslog-Einstellungen, die dem Edge zugeordnet sind, indem Sie Schritt 4 in Konfigurieren von Syslog-Einstellungen auf der Profilebene ausführen.

7 Klicken Sie auf die Schaltfläche **+**, um einen weiteren Syslog-Collector hinzuzufügen, oder klicken Sie auf **Änderungen speichern (Save Changes)**. Die Syslog-Einstellungen für den Edge werden überschrieben.

Hinweis Sie können maximal zwei Syslog-Collectors pro Segment und 10 Syslog-Collectors pro Edge konfigurieren. Wenn die Anzahl der konfigurierten Collector-Instanzen den maximal zulässigen Grenzwert erreicht, wird die Schaltfläche **+** deaktiviert.



Hinweis Basierend auf der ausgewählten Rolle exportiert der Edge die entsprechenden Protokolle in der angegebenen Schweregradstufe in den Remote-Syslog-Collector. Wenn Sie möchten, dass die von SD-WAN Orchestrator automatisch erstellen lokalen Ereignisse auf dem Syslog-Collector empfangen werden, müssen Sie Syslog auf der SD-WAN Orchestrator-Ebene mithilfe der Systemeinstellungen `log.syslog.backend` und `log.syslog.upload` konfigurieren.

Informationen zum Format einer Syslog-Nachricht für Firewall-Protokolle finden Sie unter Format der Syslog-Meldungen für Firewallprotokolle.

Nächste Schritte

Aktivieren Sie auf der Seite **Firewall** der Edge-Konfiguration die Schaltfläche **Syslog-Weiterleitung (Syslog Forwarding)**, wenn Sie Firewallprotokolle, die vom Unternehmens-SD-WAN Edges stammen, an konfigurierte Syslog-Collector-Instanzen weiterleiten möchten.

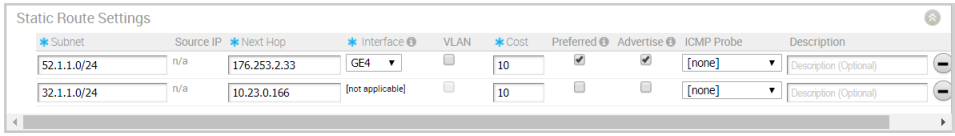
Hinweis Standardmäßig ist die Schaltfläche **Syslog-Weiterleitung (Syslog Forwarding)** auf der Seite **Firewall** der Profil- oder Edge-Konfiguration verfügbar und deaktiviert.

Weitere Informationen zu Firewalleinstellungen auf der Edge-Ebene finden Sie unter Konfigurieren der Firewall für Edges.

Konfigurieren der Einstellungen für statische Routen

Statische Routeneinstellungen (Static Route Settings) sind nützlich für spezielle Fälle, in denen statische Routen für vorhandene angeschlossene Netzwerkgeräte (z. B. Drucker) benötigt werden. Sie können zusätzliche Einstellungen für statische Routen mit den entsprechenden Symbolen rechts im Dialogfeld hinzufügen (Pluszeichen (**+**)) oder löschen (Minuszeichen (**-**)).

Einzelheiten zu den Einstellungen im Dialogfeld finden Sie in der folgenden Tabelle.



So legen Sie die Einstellungen für die statische Route fest:

1 Geben Sie das Subnetz für die Route ein.

2 Geben Sie die IP-Adresse für die Route ein.

3 Wählen Sie die WAN-Schnittstelle aus, an die die statische Route gebunden werden soll.

4 Aktivieren Sie das Kontrollkästchen **Broadcast**, um diese Route über VPN anzukündigen und anderen Edges im Netzwerk den Zugriff auf diese Ressource zu ermöglichen.

5 Fügen Sie optional eine Beschreibung für die Route hinzu.

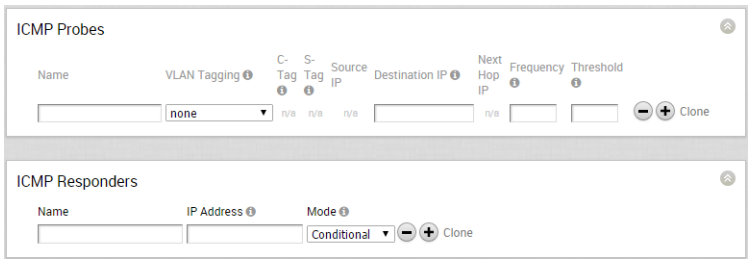
Konfigurieren von ICMP-Tests/-Respondern

ICMP-Handler sind unter Umständen notwendig, um Integration mit einem externen Router zu aktivieren, der dynamisches Routing durchführt und statusbehaftete Informationen zur Routenerreichbarkeit über VMware SD-WAN benötigt. Der Bereich **Geräteeinstellungen (Device Settings)** enthält Abschnitte zur Angabe von ICMP-Tests und -Respondern.

Bei den ICMP-Tests kann es sich um festgelegte Einstellungen für Folgendes handeln: Name, VLAN-Tagging (kein, 802.1q, 802.1ad, QinQ (0x8100) oder QinQ (0x9100)), C-Tags, S-Tags, Quell-IP/Ziel-IP/IP des nächsten Hops, Häufigkeit, mit der Ping-Anforderungen gesendet werden, sowie der Grenzwert für die Anzahl der verpassten Pings, wodurch Routen als nicht erreichbar gekennzeichnet werden.

Bei ICMP-Respondern kann es sich um festgelegte Einstellungen für Folgendes handeln: **Name**, **IP-Adresse (IP Address)** und **Modus (Mode)** (**Bedingt (Conditional)** oder **Immer (Always)**).

- **Immer (Always):** Edge reagiert immer auf ICMP-Tests.
- **Bedingt (Conditional):** Edge reagiert nur auf ICMP-Tests, wenn das SD-WAN-Overlay aktiv ist.

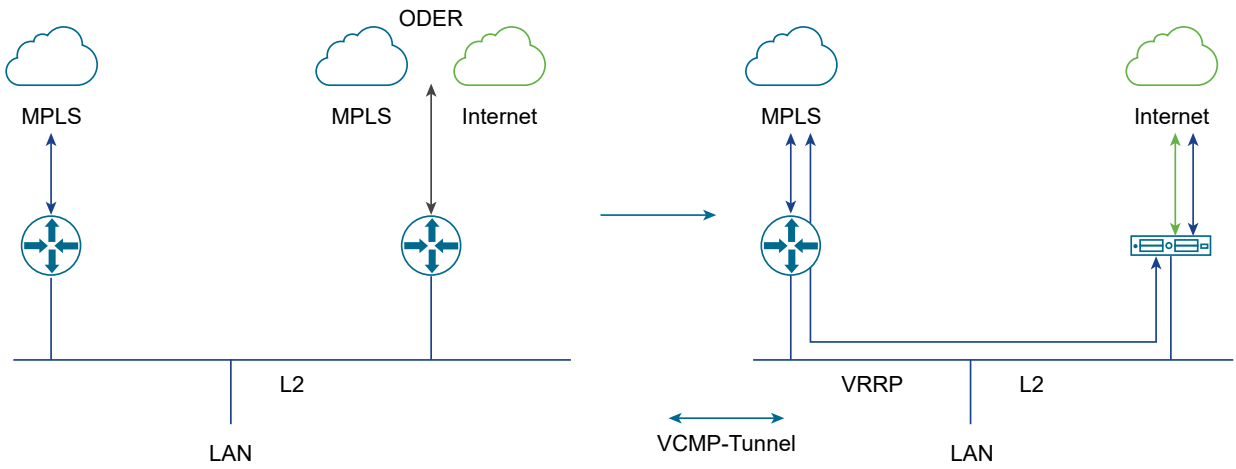


Konfigurieren von VRRP-Einstellungen

Sie können Virtual Router Redundancy Protocol (VRRP) auf einem Edge konfigurieren, um Nächster Hop-Redundanz im SD-WAN Orchestrator-Netzwerk durch Peering mit einem CE-

Router von Drittanbietern zu ermöglichen. Sie können einen Edge als VRRP-Master konfigurieren und das Gerät mit einem Router eines Drittanbieters koppeln.

Die folgende Abbildung zeigt ein Netzwerk, das mit VRRP konfiguriert ist:



Voraussetzungen

Beachten Sie vor dem Konfigurieren von VRRP die folgenden Leitlinien:

- Sie können VRRP nur zwischen dem SD-WAN Edge und einem Router von einem Drittanbieter aktivieren, der über einen L2-Switch mit demselben Subnetz verbunden ist.
- Sie können nur einen SD-WAN Edge zur VRRP-HA-Gruppe in einer Zweigstelle hinzufügen.
- Sie können Aktiv-Standby-HA und VRRP-HA nicht gleichzeitig aktivieren.
- VRRP wird auf primären gerouteten Ports, Teilschnittstellen und VLAN-Schnittstellen unterstützt.
- SD-WAN Edge muss als VRRP-Master konfiguriert werden, indem eine höhere Priorität festgelegt wird, um den Datenverkehr über SD-WAN zu steuern.
- Wenn der SD-WAN Edge als DHCP-Server konfiguriert ist, werden virtuelle IP-Adressen als Standard-Gateway-Adresse für die Clients festgelegt. Wenn Sie ein separates DHCP-Server-Relay für das LAN verwenden, muss der Administrator die virtuelle VRRP-IP-Adresse als Standard-Gatewayadresse konfigurieren.
- Wenn der DHCP-Server sowohl auf dem SD-WAN Edge als auch im Router des Drittanbieters aktiviert wird, müssen Sie den DHCP-Pool zwischen dem Edge und dem Router des Drittanbieters aufteilen, um Überschneidungen von IP-Adressen zu vermeiden.
- VRRP wird auf einer mit WAN-Overlay aktivierten Schnittstelle, die sich auf dem WAN-Link befindet, nicht unterstützt. Wenn Sie den gleichen Link für LAN verwenden möchten, erstellen Sie am besten eine Teilschnittstelle und konfigurieren VRRP auf der Teilschnittstelle.
- Sie können nur eine VRRP-Gruppe in einer Broadcast-Domäne in einem VLAN konfigurieren. Sie können keine zusätzliche VRRP-Gruppe für die sekundären IP-Adressen hinzufügen.

- Fügen Sie keinen WLAN-Link zum VRRP-fähigen VLAN hinzu. Da der Link niemals ausfallen würde, bleibt der SD-WAN Edge immer als Master erhalten.

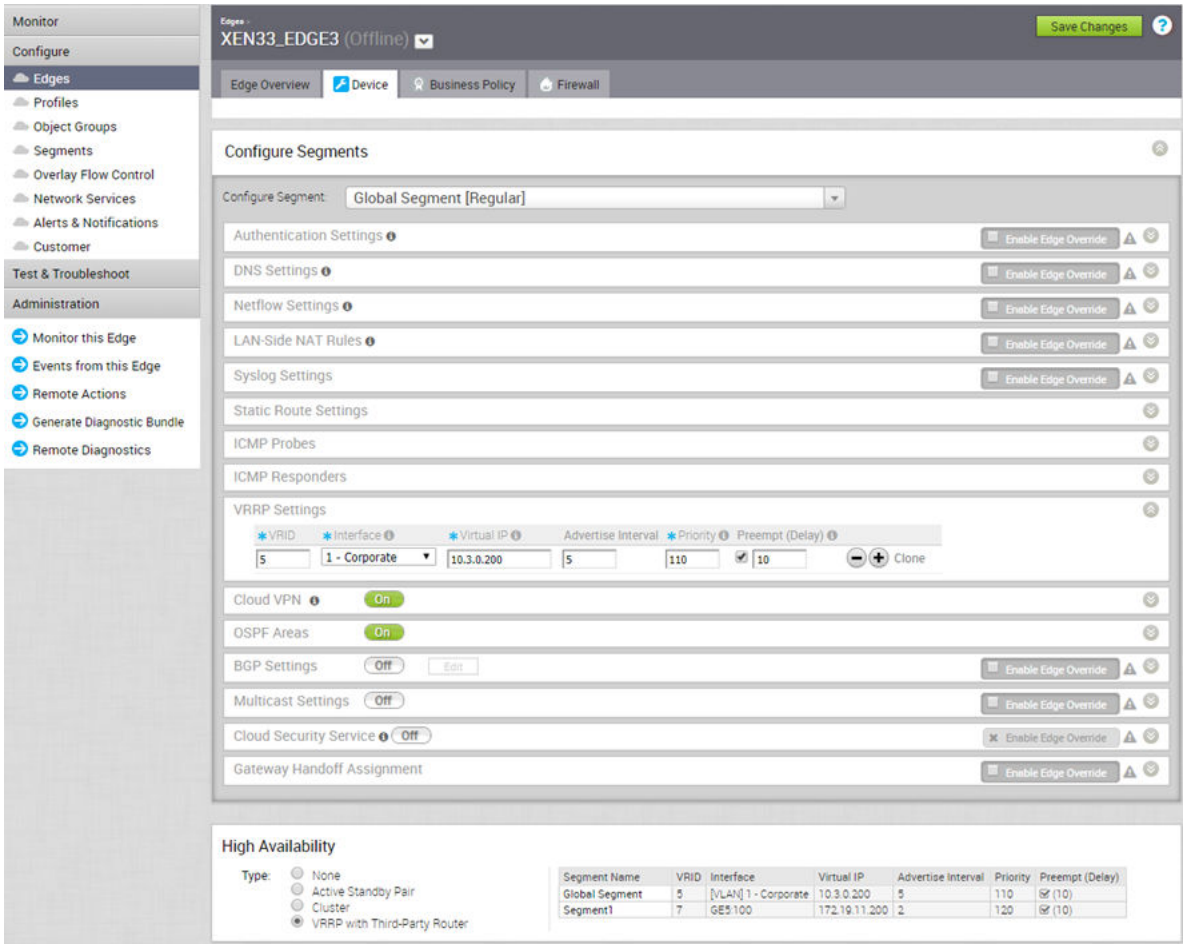
Verfahren

1 Klicken Sie im Unternehmensportal auf **Konfigurieren (Configure) > Edges**.

2 Klicken Sie entweder auf das dem Edge entsprechende **Gerätesymbol** oder auf den Edge und dann auf die Registerkarte **Gerät**.

3 Aktivieren Sie auf der Registerkarte **Gerät (Device)** unter **Hochverfügbarkeit (High Availability)** das Kontrollkästchen **VRRP mit Drittanbieter-Router (VRRP with Third-Party Router)**.

4 Konfigurieren Sie in den **VRRP-Einstellungen (VRRP Settings)** die folgenden Einstellungen:



a **VRID**: Geben Sie die VRRP-Gruppen-ID ein. Der Bereich liegt zwischen 1 und 255.

b **Schnittstelle (Interface)** – Wählen Sie eine physische oder VLAN-Schnittstelle aus der Liste aus. Das VRRP wird auf der ausgewählten Schnittstelle konfiguriert.

c **Virtuelle IP (Virtual IP)** – Geben Sie eine virtuelle IP-Adresse ein, um das VRRP-Paar zu identifizieren. Stellen Sie sicher, dass die virtuelle IP-Adresse nicht mit der IP-Adresse der Edge-Schnittstelle oder des Drittanbieter-Routers identisch ist.

d **Ankündigungsintervall** – Geben Sie das Zeitintervall ein, mit dem der VRRP-Master VRRP-Ankündigungspakete an andere Mitglieder der VRRP-Gruppe sendet.

e **Priorität (Priority)** – Um den Edge als VRRP-Master zu konfigurieren, geben Sie einen Wert ein, der den Prioritätswert des Drittanbieter-Routers überschreitet. Der Standardwert ist 100.

f **Verzögerung der Vorbelegung (Preempt Delay)** – Aktivieren Sie das Kontrollkästchen, damit der SD-WAN Edge den Drittanbieter-Router, der derzeit der Master ist, nach der angegebenen Vorbelegungsverzögerung vorbelegen kann.

5 Klicken Sie auf **Änderungen speichern (Save Changes)**.

Ergebnisse

Wenn der Edge in einem Zweigstellennetzwerk-VLAN nicht mehr verfügbar ist, werden die Clients hinter dem VLAN durch den Backup-Router umgeleitet.

Der SD-WAN Edge, der als VRRP-Master fungiert, wird zum Standard-Gateway für das Subnetz.

Wenn die Verbindung des SD-WAN Edge zu allen SD-WAN Gatewayss/Controllern unterbrochen wird, wird die VRRP-Priorität auf 10 reduziert, und der SD-WAN Gateway zieht die gelernten Routen aus dem SD-WAN Edge sowie auch die Routen in den entfernten Edges zurück. Dies führt dazu, dass der Drittanbieter-Router zum Master wird und den Datenverkehr übernimmt.

Der SD-WAN Edge verfolgt automatisch Overlay-Fehler zum SD-WAN Gateway. Wenn alle Overlay-Pfade zum SD-WAN Gateway verloren gehen, wird die VRRP-Priorität des SD-WAN Edge auf 10 reduziert.

Wenn der Edge in den VRRP-Sicherungsmodus wechselt, werden alle Pakete, die durch die virtuelle MAC gehen, von dem Edge gelöscht. Wenn der Pfad VERFÜGBAR ist, wird der Edge wieder zum VRRP-Master, sofern der Vorbelegungsmodus aktiviert ist.

Wenn VRRP auf einer gerouteten Schnittstelle konfiguriert ist, wird die Schnittstelle für den lokalen LAN-Zugriff verwendet und kann per Failover auf den Backup-Router umgeleitet werden.

VRRP wird auf einer mit WAN-Overlay aktivierten gerouteten Schnittstelle nicht unterstützt. In diesen Fällen muss eine Teilschnittstelle, die dieselbe physische Schnittstelle nutzt, für den lokalen LAN-Zugriff konfiguriert sein, damit VRRP unterstützt wird.

Wenn die LAN-Schnittstelle inaktiv ist, wechselt die VRRP-Instanz in den INIT-Status. Daraufhin sendet der SD-WAN Edge die Routenentfernungsanforderung an den SD-WAN Gateway/Controller, und alle Remote-SD-WAN Edges entfernen diese Routen. Dieses Verhalten gilt auch für die statischen Routen, die der VRRP-fähigen Schnittstelle hinzugefügt werden.

Wenn das private Overlay mit dem SD-WAN Edge-Peer-Hub vorhanden ist, wird die Route nicht aus dem Hub entfernt und kann asymmetrisches Routing verursachen. Wenn beispielsweise die Verbindung des SD-WAN-Spoke-Edge zum öffentlichen Gateway unterbrochen wird, leitet der Drittanbieter-Router die Pakete vom LAN zum SD-WAN Hub weiter. Der Hub sendet die Rückgabepakete statt an einen Drittanbieter-Router an den SD-WAN-Spoke-Edge. Als Umgehung können Sie die Funktion **SD-WAN erreichbar (SD-WAN Reachable)** aktivieren, sodass

der SD-WAN Gateway auf dem privaten Overlay erreichbar ist und den Status als VRRP-Master beibehält. Da der Internetdatenverkehr auch durch den privaten Link über das Overlay durch den SD-WAN Gateway gesteuert wird, kann es bei der Leistung oder beim Durchsatz zu Einschränkungen kommen.

Die bedingte Backhaul-Option wird verwendet, um den Internetdatenverkehr durch den Hub zu steuern. Wird hingegen in einem VRRP-fähigen SD-WAN Edge das öffentliche Overlay inaktiv, so wird der Edge zum Backup. Die bedingte Backhaul-Funktion kann daher auf einem VRRP-fähigen Edge nicht verwendet werden.

Überwachen von VRRP-Ereignissen

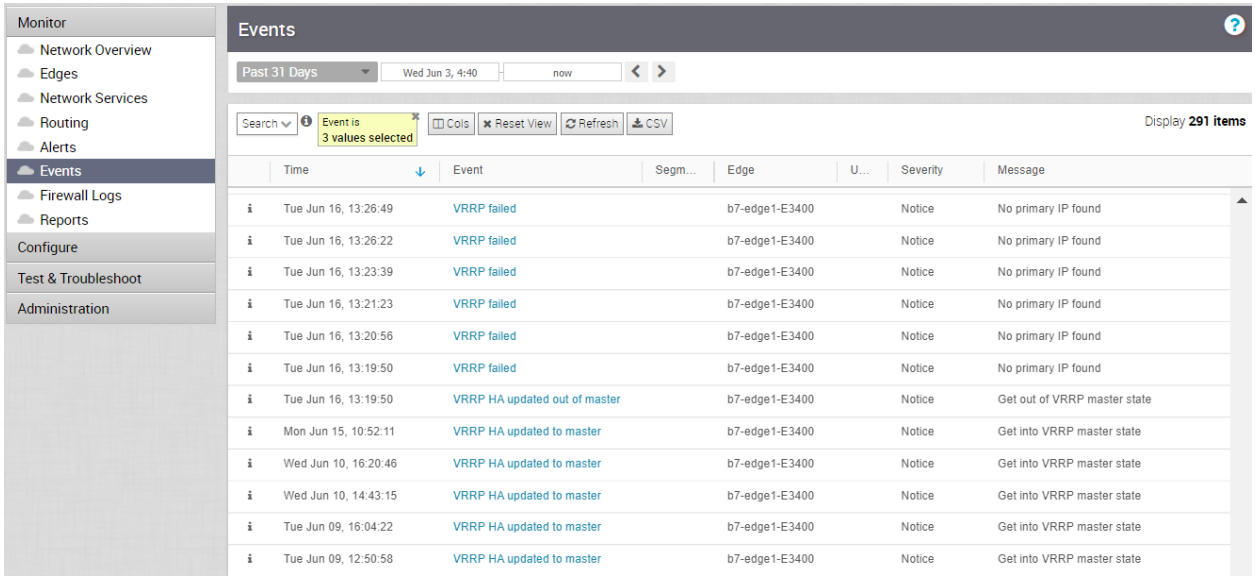
Sie können die Ereignisse im Zusammenhang mit Änderungen der VRRP-Konfiguration überwachen.

Klicken Sie im Unternehmensportal auf **Überwachen (Monitor) > Ereignisse (Events)**.

Um die Ereignisse im Zusammenhang mit VRRP anzuzeigen, können Sie die Filteroption verwenden. Klicken Sie auf den Dropdown-Pfeil neben der Option „Suchen (Search)“ und wählen Sie aus, dass nach der Spalte „Ereignis (Event)“ gefiltert werden soll. Die folgenden Ereignisse sind für VRRP verfügbar:

- VRRP HA wurde auf Master aktualisiert
- VRRP HA wurde von Master aus aktualisiert
- VRRP fehlgeschlagen

In der folgenden Abbildung sind einige der VRRP-Ereignisse dargestellt.

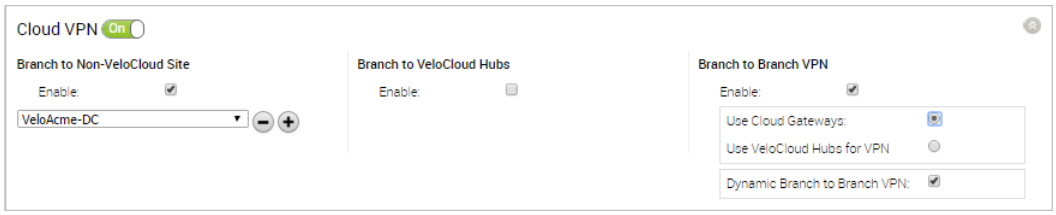


Sie können die Ereignisse auch auf der neuen Benutzeroberfläche von Orchestrator anzeigen.

Klicken Sie im Popup-Fenster auf **Neue Orchestrator-Benutzeroberfläche öffnen (Open New Orchestrator UI)** und dann auf **Neue Orchestrator-Benutzeroberfläche starten (Launch New Orchestrator UI)**. Die Benutzeroberfläche wird auf einer neuen Registerkarte geöffnet, auf der die Überwachungsoptionen angezeigt werden. Klicken Sie auf **Ereignisse (Events)**. Klicken Sie in der Suchoption auf das Filtersymbol, um die VRRP-Ereignisse zu filtern.

Edge-Cloud-VPN

Die Einstellungen für das Edge-Cloud-VPN werden von dem für den Edge ausgewählten Profil vererbt und können auf der Registerkarte **Edge-Gerät (Edge Device)** angezeigt werden. Änderungen an den Einstellungen für das Cloud-VPN können nur im verknüpften Profil vorgenommen werden.



Konfigurieren von VLAN für Edges

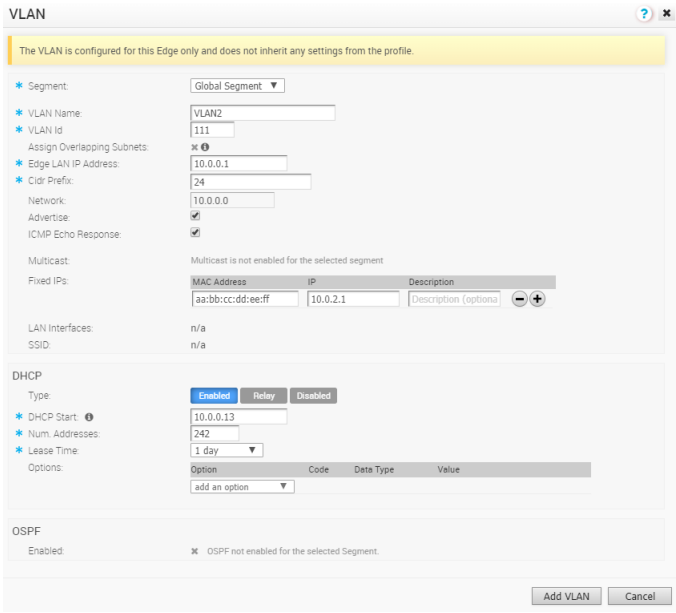
Auf der Edge-Ebene können Sie ein neues VLAN hinzufügen oder vorhandene VLAN-Einstellungen aktualisieren, die vom verknüpften Profil vererbt wurden. Bei der Konfiguration eines neuen VLAN auf Edge-Ebene können Sie mit SD-WAN Orchestrator zusätzliche, Edge-spezifische VLAN-Einstellungen konfigurieren, wie z. B. feste IP-Adressen, LAN-Schnittstellen und die SSID (Service Set Identifier) von WLAN-Schnittstellen.

Führen Sie die folgenden Schritte aus, um VLAN-Einstellungen auf Edge-Ebene zu konfigurieren:

1 Navigieren Sie in der SD-WAN Orchestrator-Instanz zu **Konfigurieren (Configure)** > **Edges**. Die Seite SD-WAN Edges wird angezeigt.

2 Wählen Sie einen Edge aus, um ein VLAN zu konfigurieren, und klicken Sie auf das Symbol in der Spalte **Gerät (Device)**. Die Seite „Geräteeinstellung (Device Setting)“ für das ausgewählte Profil wird angezeigt.

3 Zum Hinzufügen eines neuen VLAN navigieren Sie zum Bereich **VLAN konfigurieren (Configure VLAN)** und klicken Sie auf **VLAN hinzufügen (Add VLAN)**.



4 Konfigurieren Sie im Dialogfeld **VLAN** die folgenden Details:

a Wählen Sie im Dropdown-Menü **Segment** ein Profilsegment aus, um das VLAN zu konfigurieren.

b Geben Sie im Textfeld **VLAN-Name (VLAN Name)** einen eindeutigen Namen für das VLAN ein.

c Geben Sie im Textfeld **VLAN-ID (VLAN ID)** eine eindeutige ID für das VLAN ein.

d Das Feld **Überlappende Subnetze zuweisen (Assign Overlapping Subnets)**, das LAN-IP-Adressierung zulässt, wird über das zugewiesene Profil dieses Edge verwaltet. Wenn **Überlappende Subnetze zuweisen (Assign Overlapping Subnets)** aktiviert ist, werden die Werte für **Edge-LAN-IP-Adresse (Edge LAN IP Address)**, **Cidr-Präfix (Cidr Prefix)** und **DHCP** vom verknüpften Profil vererbt und sind schreibgeschützt. Die Adresse unter **Netzwerk (Network)** wird auf Basis der Subnetzmaske und des CIDR-Werts automatisch eingerichtet.

e Aktivieren Sie das Kontrollkästchen **Ankündigen (Advertise)**, um das VLAN anderen Branches im Netzwerk anzukündigen.

f Aktivieren Sie das Kontrollkästchen **ICMP-Echo-Antwort (ICMP Echo Response)**, damit das VLAN auf ICMP-Echo-Meldungen antworten kann.

g Aktivieren Sie das Kontrollkästchen **VNF-Einfügung (VNF Insertion)**, um Edge-VNF-Einfügung (Virtual Network Function) zu aktivieren.

Hinweis VNF-Einfügung erfordert, dass das ausgewählte Segment ein Dienst-VLAN aufweist. Weitere Informationen zu VNF finden Sie unter Sicherheits-VNFs.

h Geben Sie im Feld **Feste IPs (Fixed IPs)** die festen IP-Adressen ein, die an bestimmte MAC-Adressen für das VLAN gebunden sind.

i Konfigurieren Sie LAN-Schnittstellen und WLAN-SSIDs für das VLAN.

j Wenn die Funktion „Multicast“ für das ausgewählte Segment aktiviert ist, können Sie **Multicast**-Einstellungen konfigurieren, indem Sie die Kontrollkästchen **IGMP** und **PIM** aktivieren.

k Wählen Sie im Bereich **DHCP** einen der folgenden DHCP-Typen aus:

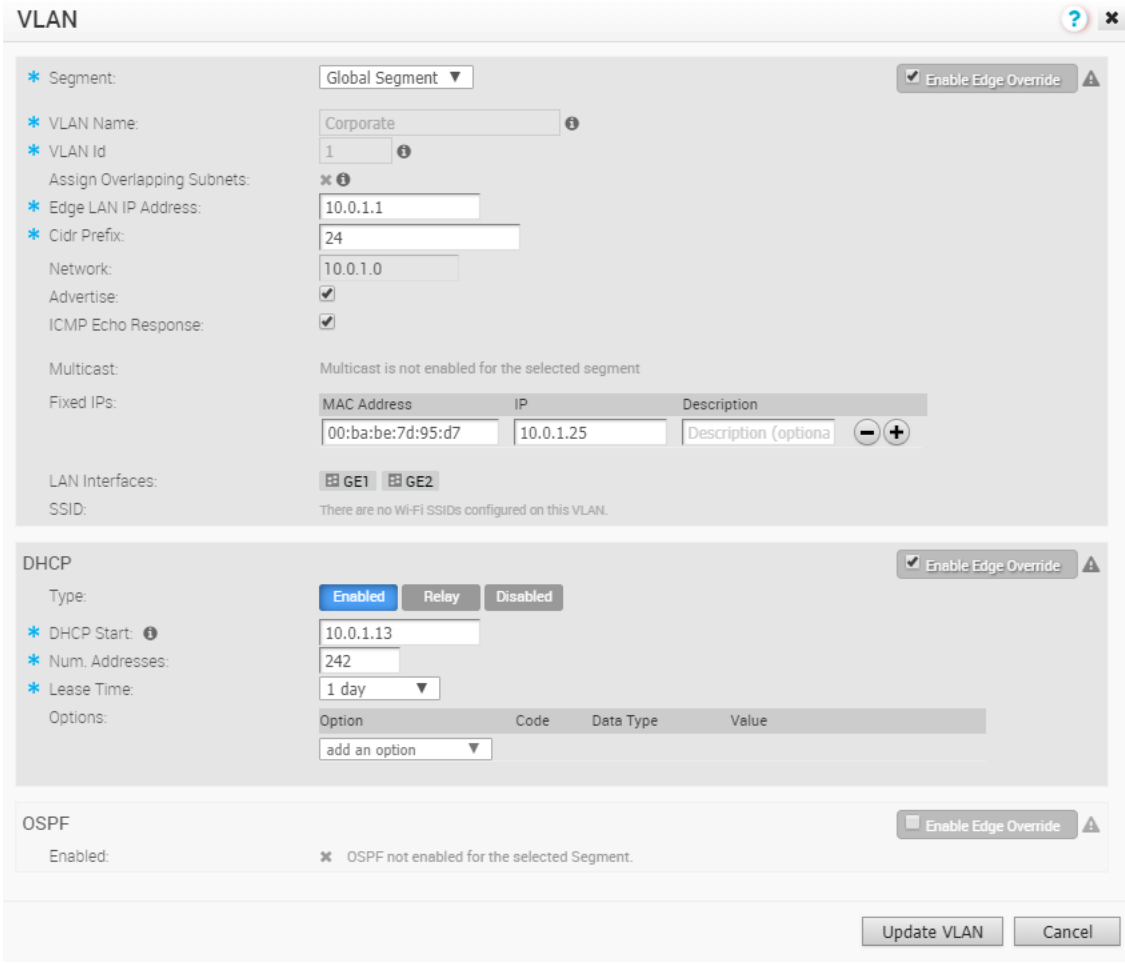
- **Aktiviert (Enabled)** – Aktiviert DHCP mit dem Edge als DHCP-Server. Wenn Sie diese Option auswählen, müssen Sie die folgenden Details angeben:
  - **DHCP starten (DHCP Start)** – Geben Sie eine gültige IP-Adresse ein, die in einem Subnetz als DHCP-Start-IP verfügbar ist.
  - **Anzahl der Adressen (Num Addresses)** – Geben Sie die Anzahl der IP-Adressen ein, die in einem Subnetz auf dem DHCP-Server zur Verfügung stehen.
  - **Lease-Dauer (Lease Time)** – Wählen Sie im Dropdown-Menü den Zeitraum aus, in dem das VLAN eine IP-Adresse verwenden kann, die dynamisch vom DHCP-Server zugewiesen wurde.

  Sie können auch eine oder mehrere DHCP-Optionen hinzufügen, wenn Sie vordefinierte Optionen angeben oder benutzerdefinierte Optionen hinzufügen.
- **Relay** – Aktiviert DHCP mit dem in einem Remote-Speicherort installierten DHCP-Relay-Agenten. Wenn Sie diese Option auswählen, können Sie die IP-Adresse eines oder mehrerer Relay-Agenten angeben.
- **Deaktiviert (Disabled)** – Deaktiviert DHCP.

l Konfigurieren Sie **OSPF**-Einstellungen, wenn die OSPF-Funktion für das ausgewählte Segment aktiviert ist.

m Klicken Sie auf **VLAN hinzufügen (Add VLAN)**.

5 Zum Aktualisieren der vom Profil vererbten VLAN-Einstellungen klicken Sie unter der Spalte **Aktionen (Actions)** auf den Link **Bearbeiten (Edit)**, der dem VLAN entspricht. Das Dialogfeld **VLAN** wird angezeigt.



6 Klicken Sie auf die Kontrollkästchen unter **Edge-Außerkraftsetzung aktivieren (Enable Edge Override)**, um die vom Profil vererbten VLAN-Einstellungen zu überschreiben.

Hinweis Sie können weder den VLAN-Namen noch die VLAN-ID des Profils überschreiben.

Informationen zum Konfigurieren von VLANs auf Profilebene finden Sie unter Konfigurieren von VLAN für Profile.

Konfigurieren von Geräteeinstellungen

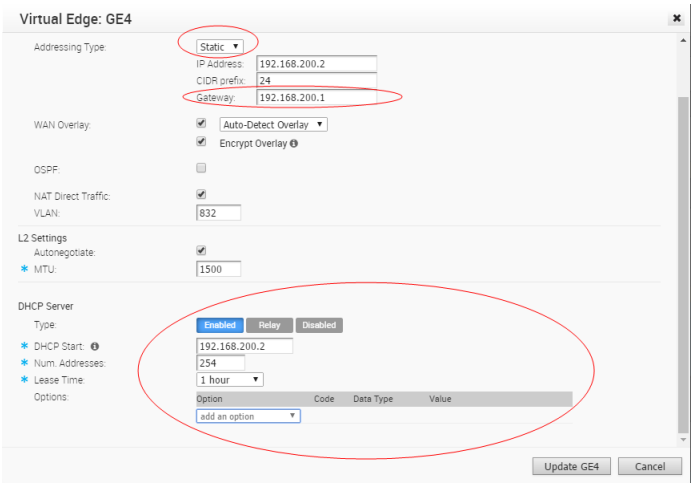
Der Bildschirm **Geräteeinstellungen (Device Settings)** für den Edge bietet die Möglichkeit, die folgenden Aufgaben auszuführen:

- Festlegen von VLAN-Einstellungen
- Außerkraftsetzen von Syslog-Einstellungen
- Außerkraftsetzen von Einstellungen für die Profilschnittstelle
- Hinzufügen eines benutzerdefinierten WAN-Overlay
- Konfigurieren von NAT für überlappendes Netzwerk

Konfigurieren von DHCP-Server auf gerouteten Schnittstellen

DHCP kann auf einer gerouteten Schnittstelle auf SD-WAN Edge konfiguriert werden. Die geroutete Schnittstelle muss mit einer statischen Adresse auf der Edge-Ebene konfiguriert werden.

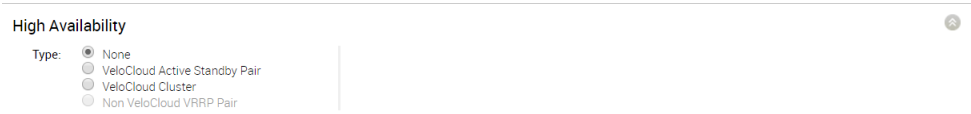
Die üblichen DHCP-Servereinstellungen können angegeben werden, einschließlich **Deaktiviert (Disabled)** (die Standardeinstellung), **Relay** (als DHCP-Relay konfigurieren) und **Aktiviert (Enabled)** (als DHCP-Server mit Optionen konfigurieren).



Hinweis Weitere Informationen finden Sie unter Tunnel-Overhead und MTU.

Hochverfügbarkeit (HA, High Availability)

Aktivieren Sie hier Hochverfügbarkeit (HA) für den Edge.



Informationen zum Setup und der Konfiguration von Hochverfügbarkeit finden Sie unter *HA-Konfiguration*.

Aktivieren von RADIUS auf einer gerouteten Schnittstelle

RADIUS kann auf jeder Schnittstelle aktiviert werden, die als geroutete Schnittstelle konfiguriert werden kann. Eine schrittweise Anleitung finden Sie in folgendem Abschnitt.

Voraussetzungen

- Ein RADIUS-Server muss konfiguriert und zum Edge hinzugefügt werden. Dieser Vorgang wird über den Bildschirm **Konfigurieren (Configure) -> Netzwerkdienste (Network Services)** im VMware SD-WAN Orchestrator ausgeführt.

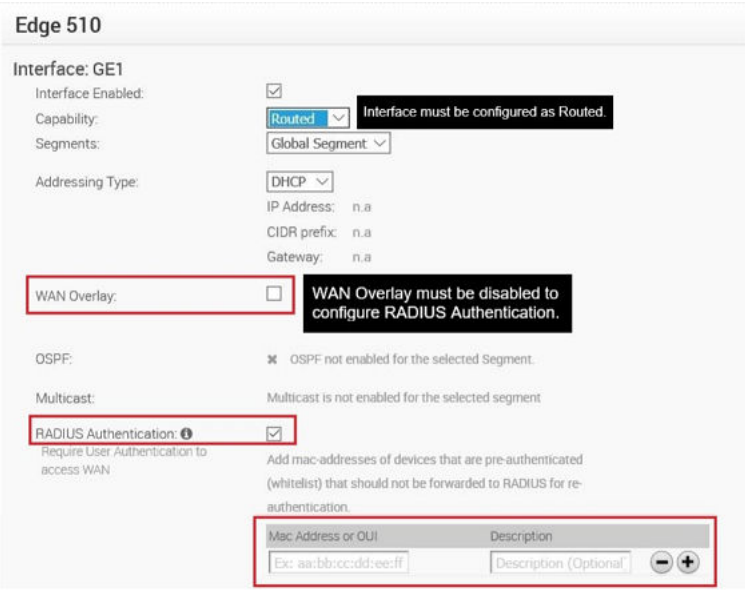
- RADIUS kann auf jeder Schnittstelle aktiviert werden, die als geroutete Schnittstelle konfiguriert werden kann. Dazu gehören die Schnittstellen für ein beliebiges Edge-Modell, ausgenommen der LAN-Ports 1-8 in den Edge-Modellen 500/520/540.

Hinweis DPDK wird auf RADIUS-fähigen Schnittstellen nicht verwendet.

Aktivieren von RADIUS auf einer gerouteten Schnittstelle

1. Navigieren Sie zu **Konfigurieren (Configure) -> Gerät (Device)** im VMware SD-WAN Orchestrator und klicken Sie auf **Bearbeiten (Edit)** für die Schnittstellen, für die RADIUS-Authentifizierung aktiviert werden soll.
2. Konfigurieren Sie den Funktionsparameter als **Weitergeleitet (Routed)**.
3. Deaktivieren Sie **WAN-Overlay (WAN Overlay)**, indem Sie die Markierung des Kontrollkästchens aufheben.
4. Aktivieren Sie **RADIUS-Authentifizierung (RADIUS Authentication)**, indem Sie das Kontrollkästchen markieren.
5. Konfigurieren Sie die Liste der zulässigen Geräte, die vorab authentifiziert wurden und für die erneute Authentifizierung nicht an RADIUS weitergeleitet werden sollen. Sie können Geräte anhand einzelner MAC-Adressen (z. B. 8c:ae:4c:fd:67:d5) sowie nach OUI (Organizationally Unique Identifier [z. B. 8c:ae:4c:00:00:00]) hinzufügen.

Hinweis Die Schnittstelle verwendet den Server, der dem Edge bereits zugewiesen ist (d. h., zwei Schnittstellen können nicht zwei verschiedene RADIUS-Server verwenden).



Konfigurieren von Edge-LAN-Überschreibungen

Die im Profil angegebenen LAN-Einstellungen können durch Aktivieren des Kontrollkästchens **Schnittstelle außer Kraft setzen (Override Interface)** überschrieben werden.

Weitere Informationen zu Konfigurationsparametern der LAN-Schnittstelle finden Sie unter Kapitel 10 Konfigurieren eines Profilgeräts.

Konfigurieren von Edge-WAN-Überschreibungen

Die im Profil angegebenen WAN-Einstellungen können durch Aktivieren des Kontrollkästchens **Schnittstelle außer Kraft setzen (Override Interface)** überschrieben werden.

Weitere Informationen zu Konfigurationsparametern der LAN-Schnittstelle finden Sie unter Kapitel 10 Konfigurieren eines Profilgeräts.

Konfigurieren der Einstellungen für Edge-WAN-Overlay

Mit den WAN-Einstellungen können Sie ein benutzerdefiniertes WAN-Overlay hinzufügen oder ändern.

Ein benutzerdefiniertes Overlay muss an eine Schnittstelle angeschlossen werden, die im Vorfeld für das WAN-Overlay konfiguriert wurde. Sie können eines der folgenden Overlays konfigurieren:

- **Privates Overlay**: Dies ist in einem privaten Netzwerk erforderlich, in dem Sie möchten, dass der Edge Overlay-VCMP-Tunnel direkt zwischen privaten IP-Adressen erstellt, die jedem Edge im privaten Netzwerk zugewiesen sind.
- **Öffentliches Overlay**: Dies ist nützlich, wenn Sie eine benutzerdefinierte VLAN- oder Quell-IP-Adresse und Gateway-Adresse für die VCMP-Tunnel festlegen möchten, um VMware SD-WAN Gateways über das Internet zu erreichen, wie durch SD-WAN Orchestrator bestimmt.

Sie können auch ein vorhandenes automatisch erkanntes WAN-Overlay ändern oder löschen, das auf einer gerouteten Schnittstelle erkannt wurde. Ein automatisch erkanntes Overlay ist nur dann verfügbar, wenn der Edge VCMP-Tunnel erfolgreich über eine geroutete Schnittstelle erstellt hat, die mit WAN-Overlay an vom SD-WAN Orchestrator designierten Gateways konfiguriert wurde.

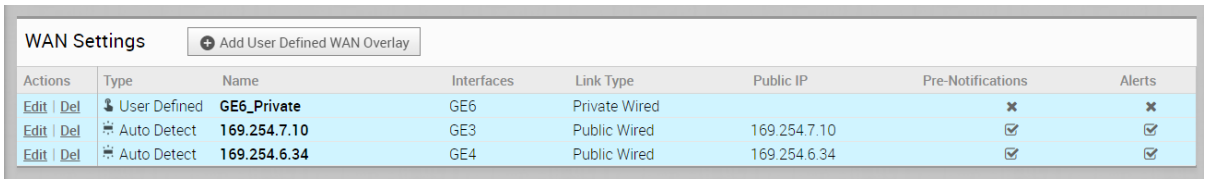
Hinweis Die unter „WAN-Einstellungen (WAN Settings)“ aufgeführten WAN-Overlays bleiben auch nach Nichtverfügbarkeit oder Nichtgebrauch einer Schnittstelle bestehen und können gelöscht werden, wenn sie nicht mehr benötigt werden.

Verfahren

1 Klicken Sie im SD-WAN Orchestrator-Portal auf **Konfigurieren (Configure) > Edges**.

2 Klicken Sie auf der Seite **Edges** entweder auf das Gerätesymbol neben einem Edge oder klicken Sie auf den Link zu dem Edge und dann auf die Registerkarte **Gerät (Device)**.

3 Scrollen Sie nach unten zum Abschnitt **WAN-Einstellungen (WAN Settings)**.



4 Klicken Sie für ein vorhandenes, automatisch erkanntes oder benutzerdefiniertes WAN-Overlay auf **Bearbeiten (Edit)**, um die Einstellungen zu ändern.

5 Um ein neues öffentliches oder privates Overlay zu erstellen, klicken Sie auf **Benutzerdefiniertes WAN-Overlay hinzufügen (Add User Defined WAN Overlay)**.

6 Wählen Sie im Fenster **Benutzerdefiniertes WAN-Overlay (User Defined WAN Overlay)** aus den folgenden verfügbaren Optionen den **Link-Typ (Link Type)** aus:

- **Öffentliches** Overlay wird über das Internet verwendet, wenn SD-WAN Cloud-Gateways, die sich im Internet befinden, erreichbar sind. Das benutzerdefinierte Overlay muss an eine Schnittstelle angehängt werden. Das öffentliche Overlay weist den Edge an, primäre und sekundäre Gateways über die Schnittstelle, an die es angehängt ist, zuzuweisen, um die Ermittlung der externen globalen NAT-Adresse zu unterstützen. Diese externe globale Adresse wird an den Orchestrator gemeldet, sodass alle anderen Edges diese externe globale Adresse verwenden, sofern sie so konfiguriert sind, dass sie VCMP-Tunnel auf dem aktuell ausgewählten Edge erstellen.

  Hinweis Standardmäßig versuchen alle gerouteten Schnittstellen, vorab zugewiesene Cloud-Gateways über das Internet **automatisch zu erkennen**, d. h. VCMP-Tunnel zu erstellen. Wenn der Versuch erfolgreich war, wird ein automatisch erkanntes öffentliches Overlay erstellt. Ein benutzerdefiniertes öffentliches Overlay ist nur erforderlich, wenn Ihr Internetdienst ein VLAN-Tag erfordert oder Sie eine andere öffentliche IP-Adresse verwenden möchten als diejenige, die der Edge über DHCP auf der der Öffentlichkeit zugewandten Schnittstelle gelernt hat.

- **Private** Overlays werden in privaten Netzwerken verwendet, z. B. in einem MPLS-Netzwerk oder einer Punkt-zu-Punkt-Verbindung. Ein privates Overlay wird wie jedes benutzerdefinierte Overlay an eine Schnittstelle angehängt und geht davon aus, dass die IP-Adresse auf der Schnittstelle, an die es angehängt ist, für alle anderen Edges im selben privaten Netzwerk routingfähig ist. Das bedeutet, dass sich keine NAT auf der WAN-Seite der Schnittstelle befindet. Wenn Sie ein privates Overlay an eine Schnittstelle anhängen, weist der Edge den Orchestrator darauf hin, dass die IP-Adresse auf der Schnittstelle für alle Remote-Edges verwendet werden sollte, die zum Erstellen von Tunneln dafür konfiguriert sind.

In den folgenden Tabellen werden die Overlay-Einstellungen beschrieben:

Tabelle 16-1. Gemeinsame Einstellungen für öffentliches und privates Overlay

Option	Beschreibung
Name	Geben Sie einen beschreibenden Namen für den öffentlichen oder privaten Link ein. Sie können auf diesen Namen verweisen, während Sie einen WAN-Link in einer Unternehmensrichtlinie auswählen. Weitere Informationen finden Sie unter Konfigurieren der Aktionslink-Steuerung.
Vorabwarnungen (Pre-Notification Alerts)	Sendet Warnungen im Zusammenhang mit dem Overlay-Netzwerk an den Operator. Sie müssen die Link-Warnungen auf der Seite **Konfigurieren (Configure) > Warnungen und Benachrichtigungen (Alerts & Notifications)** aktiviert haben, um die Warnungen zu erhalten.
Warnungen (Alerts)	Sendet Warnungen im Zusammenhang mit dem Overlay-Netzwerk an den Kunden. Sie müssen die Link-Warnungen auf der Seite **Konfigurieren (Configure) > Warnungen und Benachrichtigungen (Alerts & Notifications)** aktiviert haben, um die Warnungen zu erhalten.
Schnittstellen (Interfaces)	Wählen Sie eine oder mehrere geroutete Schnittstellen aus der Dropdown-Liste **Update-Auswahl (update selection)** aus, und das aktuelle benutzerdefinierte Overlay wird an die ausgewählte Schnittstelle angehängt. Die Liste besteht aus gerouteten Schnittstellen, bei denen das WAN-Overlay aktiviert und auf **Benutzerdefiniertes Overlay (User Defined Overlay)** festgelegt ist.

Tabelle 16-2. Einstellungen für öffentliches Overlay

Option	Beschreibung
Öffentliche IP-Adresse (Public IP Address)	Zeigt die ermittelte öffentliche IP-Adresse für ein öffentliches Overlay an. Dieses Feld wird ausgefüllt, sobald die externe globale NAT-Adresse mithilfe der Gateway-Methode ermittelt wurde.

Die folgende Abbildung zeigt ein Beispiel für Einstellungen für öffentliches Overlay:

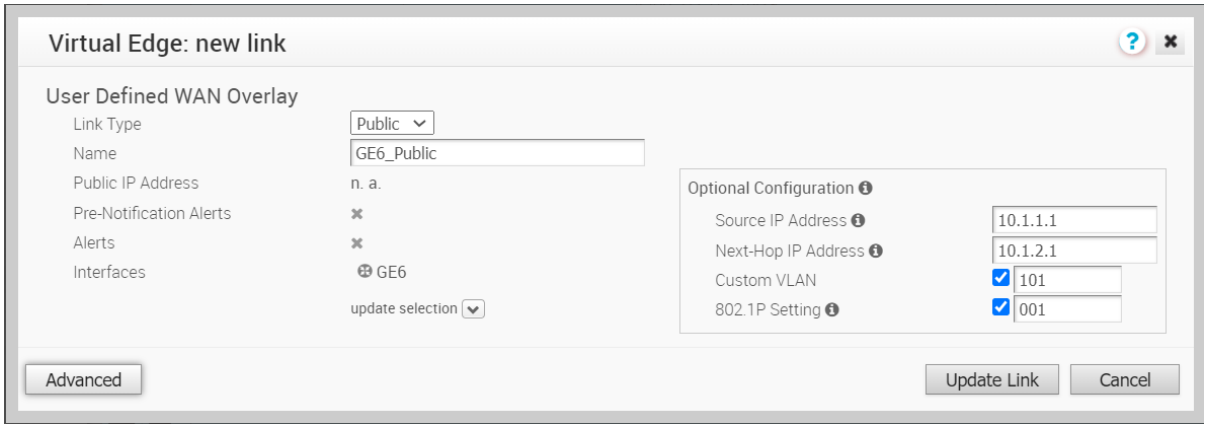

Virtual Edge: new link
User Defined WAN Overlay
Link Type
Public
Name
GE6_Public
Public IP Address
n. a.
Pre-Notification Alerts
Alerts
Interfaces
GE6
update selection
Optional Configuration
Source IP Address
10.1.1.1
Next-Hop IP Address
10.1.2.1
Custom VLAN
101
802.1P Setting
001
Advanced
Update Link
Cancel

Tabelle 16-3. Einstellungen für privates Overlay

Option	Beschreibung
SD-WAN-Dienst erreichbar (SD-WAN Service Reachable)	Wenn Sie ein privates Overlay erstellen und an ein privates WAN (z. B. MPLS-Netzwerk) anhängen, können Sie möglicherweise auch über dasselbe WAN, in der Regel durch eine Firewall im Datencenter, ins Internet gelangen. In diesem Fall wird empfohlen, die Option „SD-WAN-Dienst erreichbar (SD-WAN Service Reachable)“ zu aktivieren, da sie Folgendes bereitstellt: ■ Einen sekundären Pfad zum Internet für den Zugriff auf im Internet gehostete SD-WAN Gateways. Dies wird verwendet, wenn alle direkten Verbindungen zum Internet von diesem Edge aus fehlschlagen. ■ Einen sekundären Pfad zum Orchestrator, wenn alle direkten Verbindungen zum Internet von diesem Edge aus fehlschlagen. Die Verwaltungs-IP-Adresse, die der Edge für die Kommunikation verwendet, muss innerhalb von MPLS routingfähig sein, andernfalls müsste NAT Direct auf der privaten Schnittstelle überprüft werden, damit der Orchestrator-Datenverkehr ordnungsgemäß zurückkehrt. **Hinweis** Der SD-WAN Edge bevorzugt immer den VCMP-Tunnel, der über eine lokale Internetverbindung (kurzer Pfad) erstellt wurde, gegenüber dem über das private Netzwerk mithilfe einer Remote-Firewall erstellten VCMP-Tunnel zum Internet (langer Pfad). **Hinweis** Der Lastausgleich pro Paket oder Roundrobin wird zwischen den kurzen und langen Pfaden nicht durchgeführt. In einer Site ohne direkten öffentlichen Internetzugang ermöglicht die Option „SD-WAN-Dienst erreichbar (SD-WAN Service Reachable)“ die Nutzung des privaten WAN für private Site-zu-Site-VCMP-Tunnel und als Pfad für die Kommunikation mit einem im Internet gehosteten VMware SD-WAN-Dienst.
Öffentliche SD-WAN-Adressen (Public SD-WAN Addresses)	Wenn Sie das Kontrollkästchen **SD-WAN-Dienst erreichbar (SD-WAN Service Reachable)** aktivieren, wird eine Liste der öffentlichen IP-Adressen von SD-WAN Gateways und SD-WAN Orchestrator angezeigt, die möglicherweise über das private Netzwerk angekündigt werden müssen, wenn noch keine Standardroute über das gleiche private Netzwerk von der Firewall angekündigt wurde. Einige IP-Adressen in der Liste, wie Gateways, können sich im Laufe der Zeit ändern.

Die folgende Abbildung zeigt ein Beispiel für Einstellungen für privates Overlay:

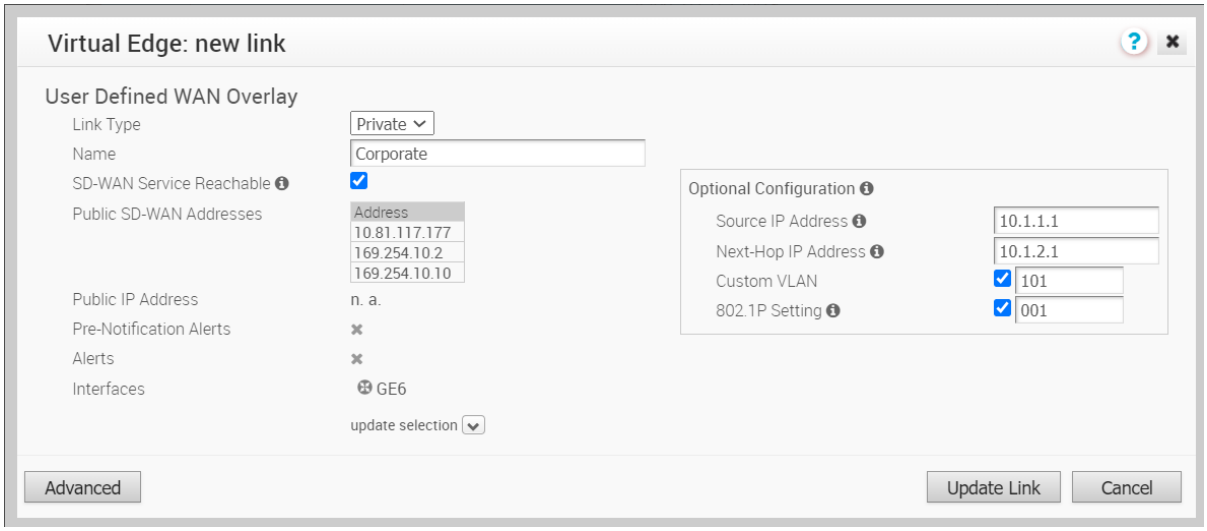


Tabelle 16-4. Optionale Konfiguration

Option	Beschreibung
Quell-IP-Adresse (Source IP Address)	Dies ist die IP-Adresse der Raw-Socket-Quelle, die für VCMP-Tunnelpakete verwendet wird, welche von der Schnittstelle stammen, an die das aktuelle Overlay angehängt ist. Die Quell-IP-Adresse muss nirgendwo vorkonfiguriert sein, doch sie muss zu und von der ausgewählten Schnittstelle routingfähig sein.
IP-Adresse für nächsten Hop (Next-Hop IP Address)	Geben Sie die IP-Adresse des nächsten Hops ein, an die die Pakete weitergeleitet werden sollen, die von der im Feld **Quell-IP-Adresse (Source IP Address)** angegebenen IP-Adresse der Raw-Socket-Quelle stammen.

Tabelle 16-4. Optionale Konfiguration (Fortsetzung)

Option	Beschreibung
Benutzerdefiniertes VLAN (Custom VLAN)	Aktivieren Sie das Kontrollkästchen, um das benutzerdefinierte VLAN zu aktivieren und die VLAN-ID einzugeben. Der Bereich liegt zwischen 2 und 4094. Diese Option wendet das VLAN-Tag auf die Pakete an, die von der Quell-IP-Adresse eines VCMP-Tunnels von der Schnittstelle stammen, an die das aktuelle Overlay angehängt ist.
802.1P-Setting (802.1P Setting)	Setzt 802.1p-PCP-Bits auf Frames, die die Schnittstelle verlassen, an die das aktuelle Overlay angehängt ist. Diese Einstellung ist nur für ein bestimmtes VLAN verfügbar. PCP-Prioritätswerte sind eine 3-stellige Binärzahl. Der Bereich liegt zwischen 000 und 111, und der Standardwert ist 000. Dieses Kontrollkästchen ist nur verfügbar, wenn die Systemeigenschaft **session.options.enable8021PConfiguration** auf „True“ gesetzt sein muss. Standardmäßig ist dieser Wert auf „False“ festgelegt. Falls diese Option für Sie nicht verfügbar ist, wenden Sie sich an den VMware SD-WAN-Support Ihres Operations-Teams, um die Einstellung zu aktivieren.

Klicken Sie auf **Erweitert (Advanced)**, um die folgenden Einstellungen zu konfigurieren:

Tabelle 16-5. Erweiterte Einstellungen für öffentliches und privates Overlay

Option	Beschreibung
Messung der Bandbreite (Bandwidth Measurement)	Wählen Sie aus den folgenden Optionen eine Methode zur Messung der Bandbreite aus: ■ **Messung der Bandbreite (Langsamer Start) (Measure Bandwidth (Slow Start))**: Wenn die Messung der Standardbandbreite falsche Ergebnisse liefert, kann dies auf eine Drosselung des ISPs zurückzuführen sein. Um dieses Verhalten zu überwinden, wählen Sie diese Option für einen anhaltend langsamen Burst von UDP-Verkehr, gefolgt von einem größeren Burst. ■ **Messung der Bandbreite (Burst-Modus) (Measure Bandwidth (Burst Mode))**: Wählen Sie diese Option aus, um kurze Bursts von UDP-Datenverkehr zu einem SD-WAN Gateway für öffentliche Links oder zum Peer für private Verbindungen durchzuführen, um die Bandbreite der Verbindung zu bewerten. ■ **Nicht messen (manuell definieren) (Do Not Measure (define manually))**: Wählen Sie diese Option aus, um die Bandbreite manuell zu konfigurieren. Dies wird aus folgenden Gründen für die Hub-Sites empfohlen: a Hub-Sites können in der Regel nur an entfernten Zweigstellen messen, die langsamere Verbindungen als der Hub haben. b Wenn ein Hub-Edge ausfällt und einen dynamischen Bandbreitenmessmodus verwendet, kann dies zu einer zusätzlichen Verzögerung beim Wiederherstellen des Online-Status des Hub-Edge führen, während sie die verfügbare Bandbreite erneut misst.
Upstream-Bandbreite (Upstream Bandwidth)	Geben Sie die Upstream-Bandbreite in MBit/s ein. Diese Option steht nur dann zur Verfügung, wenn Sie „Nicht messen (manuell definieren) (Do Not Measure (define manually))“ auswählen.
Downstream-Bandbreite (Downstream Bandwidth)	Geben Sie die Downstream-Bandbreite in MBit/s ein. Diese Option steht nur dann zur Verfügung, wenn Sie „Nicht messen (manuell definieren) (Do Not Measure (define manually))“ auswählen.

Tabelle 16-5. Erweiterte Einstellungen für öffentliches und privates Overlay (Fortsetzung)

Option	Beschreibung
Dynamische Bandbreitenanpassung (Dynamic Bandwidth Adjustment)	Die dynamische Bandbreitenanpassung versucht, die verfügbare Verbindungsbandbreite basierend auf Paketverlust dynamisch anzupassen, und ist für die Verwendung mit Wireless-Breitbanddiensten vorgesehen, bei denen die Bandbreite plötzlich abnehmen kann. **Hinweis** Diese Option funktioniert nur für WAN-Links ohne latenten Verlust, so dass es möglich ist, routinemäßige Paketverluste fälschlicherweise als Überlastung zu interpretieren. In einigen Fällen kann dies dazu führen, dass die verfügbare Bandbreite für WAN-Links mit nicht zusammenhängendem Paketverlust auf 2 Mbit/s absinkt. **Hinweis** Diese Konfiguration wird nicht für Edges mit Softwareversion bis 3.3.x empfohlen. Sie können diese Option für Edges mit Version 3.4 oder höher konfigurieren.
Nur als Sicherung verwenden (Use as Backup Only)	Mit dieser Option wird die Schnittstelle, an die dieses WAN-Overlay angehängt ist, in den Backup-Modus versetzt. Dies bedeutet, dass die VCMP-Tunnel entfernt werden und die Schnittstelle nur verwendet werden darf, wenn Tunnel wieder aufgebaut werden und alle anderen von diesem Edge ausgehenden Pfade nicht verfügbar sind. Nur eine Schnittstelle auf einem Edge kann in den Backup-Modus versetzt werden. Wenn aktiviert, wird die Schnittstelle auf der Seite **Überwachen (Monitor) > Edges** als **Cloud-Status: Standby (Cloud Status: standby)** angezeigt. **Hinweis** Verwenden Sie diese Option, um den Bandbreitenverbrauch von Benutzerdaten und SD-WAN-Leistungsmessungen für einen 4G- oder LTE-Dienst zu reduzieren. Failover-Zeiten sind jedoch langsamer als bei einem Link, der sich nicht im Backup-Modus befindet und bei dem die Unternehmensrichtlinie zur Reduzierung des Bandbreitenverbrauchs angewendet wird. Verwenden Sie diese Funktion nicht, wenn der Edge als Hub verwendet wird oder Teil eines Clusters ist.

Tabelle 16-5. Erweiterte Einstellungen für öffentliches und privates Overlay (Fortsetzung)

Option	Beschreibung
MTU	Der SD-WAN Edge führt die MTU-Pfaderkennung durch, und der erkannte MTU-Wert wird in diesem Feld aktualisiert. Die meisten kabelgebundenen Netzwerke unterstützen 1500 Byte, während 4G-Netzwerke, die VoLTE unterstützen, in der Regel maximal 1358 Byte ermöglichen. Eine MTU-Einstellung 1300 Byte wird nicht empfohlen, da dies zu einem Framing Overhead führen kann. Es ist nicht notwendig, die MTU festzulegen, es sei denn, die MTU-Pfaderkennung ist ausgefallen. Ob die MTU groß ist, können Sie auf der Seite **Remote-Diagnose (Remote Diagnostics) > Pfade auflisten (List Paths)** feststellen, wenn die VCMP-Tunnel (Pfade) für die Schnittstelle nie stabil werden und wiederholt einen NICHT VERWENDBAREN Status mit Paketverlusten von über 25 % erreichen. Da die MTU während des Bandbreitentests auf jedem Pfad allmählich ansteigt, gehen alle Pakete, die größer sind als die Netzwerk-MTU, verloren, wenn die konfigurierte MTU größer als die Netzwerk-MTU ist. Das führt zu schwerwiegendem Paketverlust auf dem Pfad. Weitere Informationen finden Sie unter Tunnel-Overhead und MTU.
Overhead-Bytes (Overhead Bytes)	Geben Sie einen Wert für die Overhead-Bandbreite in Byte ein. Dies ist eine Option zur Angabe des zusätzlichen L2-Framing-Overheads, der im WAN-Pfad vorhanden ist. Wenn Sie die Overhead-Bytes konfigurieren, werden die Bytes zusätzlich zur tatsächlichen Paketlänge durch den QoS-Zeitplan für jedes Paket berücksichtigt. Dadurch wird sichergestellt, dass die Verbindungsbandbreite nicht durch einen vorgelagerten L2-Framing-Overhead überbeansprucht wird.

Tabelle 16-6. Erweiterte Einstellungen für öffentliches Overlay

Option	Beschreibung
UDP Hole Punching	Wenn ein SD-WAN-Overlay von Zweigstelle zu Zweigstelle erforderlich ist und Zweigstellen-Edges hinter NAT-Geräten bereitgestellt werden, d. h. wenn sich das NAT-Gerät auf der WAN-Seite des Edge befindet, wird der direkte VCMP-Tunnel auf UDP/2426 wahrscheinlich nicht verfügbar, wenn die NAT-Geräte nicht so konfiguriert wurden, dass eingehende VCMP-Tunnel auf UDP-Port 2426 von anderen Edges zugelassen werden. Über **Zweigstelle-zu-Zweigstelle-VPN (Branch to Branch VPN)** können Sie Zweigstelle-zu-Zweigstelle-Tunnel aktivieren. Weitere Informationen finden Sie unter Konfigurieren eines Zweigstelle-zu-Zweigstelle-VPNs und Edge-Cloud-VPN. Anhand der **Remote-Diagnose > Pfade auflisten (List Paths)** können Sie überprüfen, ob ein Edge einen Tunnel zu einem anderen Edge erstellt hat. UDP Hole Punching versucht eine Umgehung zu bieten, wenn NAT-Geräte eingehende Verbindungen blockieren. Diese Methode ist jedoch nicht in allen Szenarien oder bei allen Arten von NATs anwendbar, da die NAT-Betriebseigenschaften nicht standardisiert sind. Wenn Sie UDP Hole Punching auf einer Edge-Overlay-Schnittstelle aktivieren, werden alle Remote-Edges angewiesen, die über das SD-WAN Gateway erkannte öffentliche IP der NAT und den erkannten dynamischen Quellport der NAT als Ziel-IP und Zielport für das Erstellen eines VCMP-Tunnels zu dieser Edge-Overlay-Schnittstelle zu verwenden. **Hinweis** Konfigurieren Sie vor der Aktivierung von UDP Hole Punching erst das Zweigstellen-NAT-Gerät, um eingehendes UDP/2426 mit Portweiterleitung an die private IP-Adresse des Edge zuzulassen, oder versetzen Sie das NAT-Gerät, bei dem es sich in der Regel um einen Router oder ein Modem handelt, in den Überbrückungsmodus. Verwenden Sie UDP Hole Punching nur als letztes Mittel, da es mit Firewalls, symmetrischen NAT-Geräten, 4G/LTE-Netzwerken aufgrund von CGNAT und den meisten modernen NAT-Geräten nicht funktioniert. Durch UDP Hole Punching können zusätzliche Konnektivitätsprobleme auftreten, da die Remote-Sites versuchen, den neuen dynamischen UDP-Port für VCMP-Tunnel zu verwenden.
Typ	Wenn Sie eine Unternehmensrichtlinie für einen Edge konfigurieren, können Sie die **Link-Steuerung (Link-Steering)** auswählen, um eine der folgenden **Transportgruppe (Transport Group)** zu bevorzugen:

Tabelle 16-6. Erweiterte Einstellungen für öffentliches Overlay (Fortsetzung)

Option	Beschreibung
	Öffentlich verkabelt (Public Wired), Öffentlich drahtlos (Public Wireless) oder Privat verkabelt (Private Wired). Weitere Informationen finden Sie unter Konfigurieren der Aktionslink-Steuerung. Wählen Sie **Wired (Verkabelt)** oder **Wireless (Drahtlos)** aus, um das Overlay in eine öffentliche verkabelte oder in eine drahtlose Transportgruppe zu versetzen.

Die folgende Abbildung zeigt ein Beispiel für erweiterte Einstellungen für ein öffentliches Overlay:

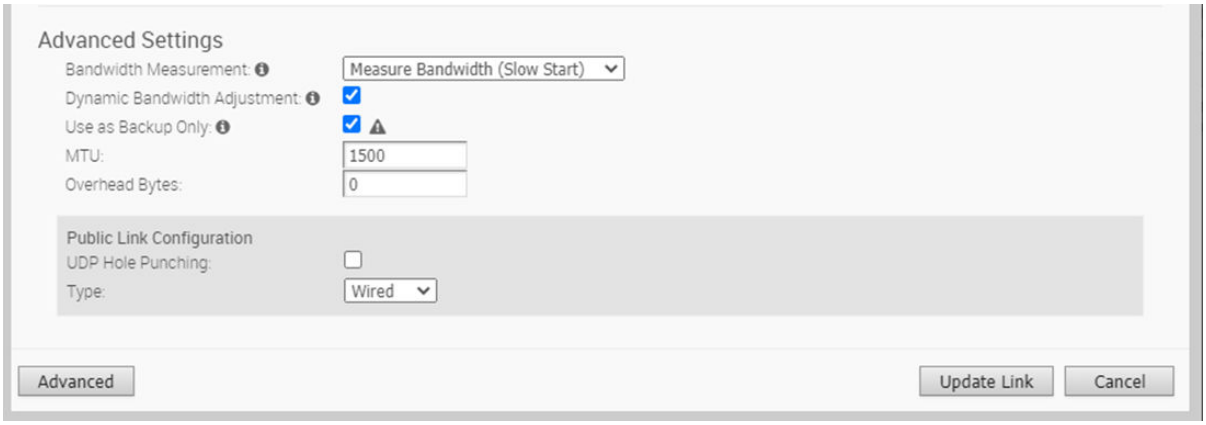


Tabelle 16-7. Erweiterte Einstellungen für privates Overlay

Option	Beschreibung
Privater Netzwerkname (Private Network Name)	Wenn Sie über mehr als ein privates Netzwerk verfügen und zwischen diesen unterscheiden möchten, um sicherzustellen, dass die Edges Tunnelverbindungen nur zu Edges in demselben privaten Netzwerk verwenden, können Sie einen privaten Netzwerknamen festlegen und das Overlay daran anhängen. Dadurch wird das Tunneling zu Edges in einem anderen, für sie unerreichbaren privaten Netzwerk verhindert. Darüber hinaus sollten Sie die Edges an anderen Standorten in diesem privaten Netzwerk konfigurieren, um denselben privaten Netzwerknamen zu nutzen. Beispiel: Edge1 GE1 wird an das *private Netzwerk A* angehängt. Verwenden Sie das *private Netzwerk A* für das an GE1 angehängte private Overlay. Edge1 GE2 wird an das *private Netzwerk B* angehängt. Verwenden Sie das *private Netzwerk B* für das an GE2 angehängte private Overlay. Wiederholen Sie die gleiche Anhängung und Benennung für Edge2. Wenn Sie Zweigstelle zu Zweigstelle aktivieren oder wenn Edge2 eine Hub-Site ist: ■ Edge1 GE1 versucht eine Verbindung zu Edge2 GE1 herzustellen anstatt zu GE2. ■ Edge1 GE2 versucht eine Verbindung zu Edge2 GE2 herzustellen anstatt zu GE1.
Konfiguration eines statischen SLA (Configure Static SLA)	Erzwingt, dass das Overlay von der Annahme ausgeht, dass die festgelegten SLA-Parameter die tatsächlichen SLA-Werte für den Pfad sind. Auf diesem Overlay wird keine dynamische Messung von Paketverlust, Latenz oder Jitter durchgeführt. Der Quality of Experience-Bericht verwendet diese Werte für seine grün-gelbe-rote Färbung im Verhältnis zu den Schwellenwerten. **Hinweis** Statische SLA-Konfiguration wird ab Version 3.4 nicht unterstützt. Von der Verwendung dieser Option wird abgeraten, da die dynamische Messung von Paketverlust, Latenz und Jitter bessere Ergebnisse liefert.

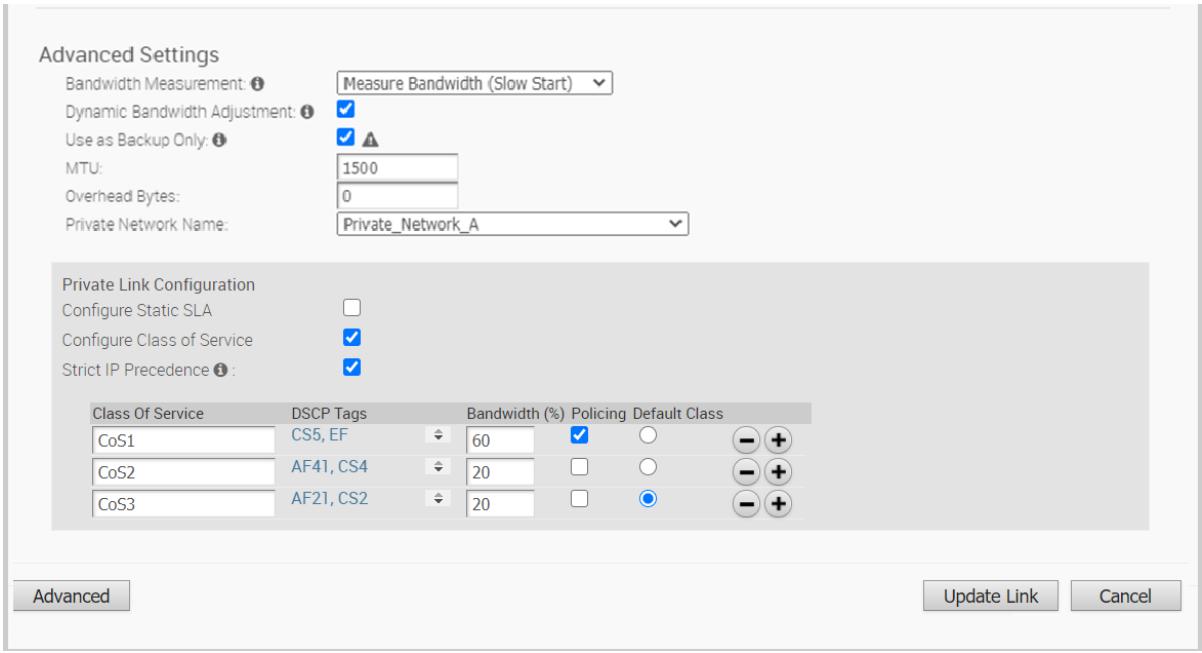
Tabelle 16-7. Erweiterte Einstellungen für privates Overlay (Fortsetzung)

Option	Beschreibung
Dienstklasse konfigurieren (Configure Class of Service)	SD-WAN Edges können den Datenverkehr priorisieren und eine 3x3-Dienstgüteklassenmatrix sowohl über das Internet als auch über private Netzwerke bereitstellen. Einige MPLS-Netzwerke umfassen jedoch ihre eigenen Dienstgüteklassen (Quality of Service, QoS) mit jeweils spezifischen Eigenschaften wie garantierten Raten, Grenzwerten für Raten, Paketverlustwahrscheinlichkeit usw. Anhand dieser Option kann der Edge die verfügbare QoS-Bandbreite des privaten Netzwerks ermitteln und das private Overlay auf einer bestimmten Schnittstelle überwachen. **Hinweis** Äußere DSCP-Tags müssen in der Unternehmensrichtlinie pro Anwendung/Regel festgelegt werden, und in dieser Funktion stimmt jede Dienstklassenzeile mit den in der Unternehmensrichtlinie festgelegten DSCP-Tags überein. Konfigurieren Sie nach dem Aktivieren dieses Kontrollkästchens die folgenden Einstellungen: ■ **Dienstklasse (Class of Service)**: Geben Sie einen beschreibenden Namen für die Dienstklasse ein. Sie können auf diesen Namen verweisen, während Sie einen WAN-Link in einer Unternehmensrichtlinie auswählen. Weitere Informationen finden Sie unter Konfigurieren der Aktionslink-Steuerung. ■ **DSCP-Tags**: Die Dienstklasse stimmt mit den hier festgelegten DSCP-Tags überein. DSCP-Tags werden jeder Anwendung mithilfe der Unternehmensrichtlinie zugewiesen. ■ **Bandbreite**: Prozentsatz der verfügbaren Bandbreite der Schnittstelle für Übertragungen/Uploads für diese Klasse. Dieser richtet sich nach der garantierten Dienstgütenklassenbandbreite des privaten Netzwerks. ■ **Überwachung (Policing)**: Diese Option überwacht die vom Datenverkehr in der Dienstklasse verwendete Bandbreite und begrenzt den Datenverkehr, wenn der Datenverkehr die Bandbreite überschreitet. ■ **Standardklasse (Default Class)**: Wenn der Datenverkehr nicht unter eine der definierten Klassen fällt, wird der Datenverkehr der Standard-Dienstklasse zugeordnet. Weitere Informationen zur Dienstklasse finden Sie unter Konfigurieren von MPLS-CoS.
Strenger IP-Vorrang (Strict IP precedence)	Dieses Kontrollkästchen ist verfügbar, wenn Sie das Kontrollkästchen **Dienstklasse konfigurieren (Configure Class of Service)** aktivieren.

Tabelle 16-7. Erweiterte Einstellungen für privates Overlay (Fortsetzung)

Option	Beschreibung
	Bei Aktivierung dieser Option werden 8 VCMP-Unterpfade erstellt, die den 8 IP-Vorrang-Bit entsprechen. Verwenden Sie diese Option, wenn Sie die Dienstklassen in weniger Klassen im Netzwerk Ihres Dienstanbieters zusammenfassen möchten. Diese Option ist standardmäßig deaktiviert, und die VCMP-Unterpfade werden für die genaue Menge der konfigurierten Dienstklassen erstellt. Die Zusammenfassung wird nicht angewendet.

Die folgende Abbildung zeigt ein Beispiel für erweiterte Einstellungen für ein privates Overlay:



7 Klicken Sie auf **Link aktualisieren (Update Link)**, um die Einstellungen zu speichern.

Konfigurieren von MPLS-CoS

Sie können den Datenverkehr verwalten, indem Sie die Dienstklasse (Class of Service, CoS) in einem privaten WAN-Link definieren. Sie können ähnliche Datenverkehrstypen wie eine Klasse gruppieren. Die CoS behandelt jede Klasse mit ihrer Dienstpriorität.

Für jeden Edge, der aus privaten WAN-Links besteht, können Sie die Dienstklasse definieren.

1 Klicken Sie im Unternehmensportal auf **Konfigurieren (Configure) > Edges**.

2 Klicken Sie entweder auf das Gerätesymbol neben einem Edge oder klicken Sie auf den Link zum Edge und dann auf die Registerkarte **Gerät (Device)**.

3 Klicken Sie im Abschnitt **WAN-Einstellungen (WAN Settings)** auf **Benutzerdefiniertes WAN-Overlay hinzufügen (Add User Defined WAN Overlay)** und wählen Sie den Linktyp **Privat (Private)**.

4 Sie können die Dienstklasse auch für einen vorhandenen privaten Link definieren, indem Sie auf **Bearbeiten (Edit)** klicken.

5 Klicken Sie in den **WAN-Overlay (WAN Overlay)**-Einstellungen auf **Erweitert (Advanced)** und aktivieren Sie das Kontrollkästchen **Dienstklasse konfigurieren (Configure Class of Service)**. Bei Aktivierung dieser Option werden die folgenden Einstellungen angezeigt und entsprechend konfiguriert. Sie können auf das Pluszeichen (**+**) klicken, um mehrere Dienstklassen hinzuzufügen.

- **Strenger IP-Vorrang (Strict IP precedence)**: Aktivieren Sie dieses Kontrollfach, um strengen IP-Vorrang durchzusetzen.

  Bei Aktivierung dieser Option werden 8 VCMP-Unterpfade erstellt, die den 8 IP-Vorrang-Bit entsprechen. Verwenden Sie diese Option, wenn Sie die Dienstklassen in weniger Klassen im Netzwerk Ihres Dienstanbieters zusammenfassen möchten.

  Diese Option ist standardmäßig deaktiviert, und die VCMP-Unterpfade werden für die genaue Menge der konfigurierten Dienstklassen erstellt. Die Zusammenfassung wird nicht angewendet.

- **Dienstklasse (Class of Service)**: Geben Sie einen beschreibenden Namen für die Dienstklasse ein. Der Name kann eine Kombination aus alphanumerischen und Sonderzeichen sein.

- **DSCP-Tags (DSCP Tags)**: Klicken Sie auf **Festlegen (Set)**, um der Dienstklasse DSCP-Tags zuzuweisen. Sie können mehrere DSCP-Tags aus der verfügbaren Liste auswählen.

  Hinweis Sie sollten DSCP-Tags mit gleicher IP-Priorität zur gleichen Dienstklasse zuordnen. Eine CoS-Warteschlange kann ein Aggregat aus vielen Klassen sein, aber DSCP-Werte derselben Klasse können nicht Teil von Warteschlangen für mehrere Klassen sein.

  Beispielsweise kann die folgende Gruppe von DSCP-Tags nicht über mehrere Warteschlangen verteilt werden:

  - CS1 und AF11 zu AF14
  - CS2 und AF21 zu AF24
  - CS3 und AF31 zu AF34
  - CS4 und AF41 zu AF44

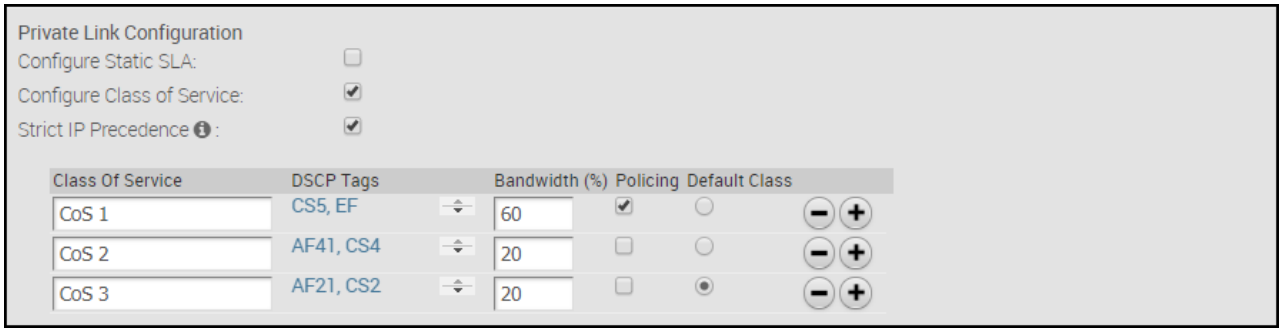
- **Bandbreite (Bandwidth)**: Geben Sie einen Wert in Prozent für den Datenverkehr ein, der der CoS zugeordnet ist. Dieser Wert weist der Klasse eine Gewichtung zu. Der eingehende Datenverkehr wird basierend auf der dazugehörigen Gewichtung verarbeitet. Wenn mehrere Dienstklassen vorhanden sind, sollte der Gesamtwert der Bandbreite bis zu 100 betragen.

- **Überwachung (Policing)**: Aktivieren Sie das Kontrollkästchen, um die klassenbasierte Überwachung zu aktivieren. Diese Option überwacht die Bandbreite, die vom Verkehrsfluss in der Dienstklasse verwendet wird, und wenn der Verkehr die Bandbreite überschreitet, überwacht sie den Datenverkehr.
- **Standardklasse (Default Class)**: Klicken Sie, um die entsprechende Dienstklasse als Standard festzulegen. Wenn der eingehende Datenverkehr nicht unter eine der definierten Klassen fällt, wird der Datenverkehr mit der Standard-CoS verknüpft.

6 Klicken Sie auf **Link aktualisieren (Update Link)**, um die Einstellungen zu speichern.

Das folgende Beispiel zeigt mehrere Dienstklassen mit unterschiedlichen Gruppen von DSCP-Tags.

Dienstklasse	Beschreibung	DSCP-Tags	Überwachung
CoS1	Audio	CS5, EF	Aktiviert
CoS2	Video	AF41, CS4	Deaktiviert
CoS3	Dateiübertragung	AF21, CS2	Deaktiviert



Weitere Informationen zu den Einstellungen für WAN-Overlay finden Sie unter Konfigurieren der Einstellungen für Edge-WAN-Overlay.

Erreichbarkeit des SD-WAN-Diensts über MPLS

Ein Edge mit ausschließlich privaten MPLS-Links kann den Orchestrator und die Gateways in der Public Cloud über die Option „SD-WAN-Dienst erreichbar (SD-WAN Service Reachable)“ erreichen.

In einer Site ohne direkten öffentlichen Internetzugang ermöglicht die Option „SD-WAN-Dienst erreichbar (SD-WAN Service Reachable)“ die Nutzung des privaten WAN für private Site-zu-Site-VCMP-Tunnel und als Pfad für die Kommunikation mit einem im Internet gehosteten VMware SD-WAN-Dienst.

Bei hybriden Umgebungen, die über Links vom Typ „Nur MPLS“ verfügen oder ein Failover zu MPLS-Links erfordern, können Sie die Option „SD-WAN-Dienst erreichbar (SD-WAN Service Reachable)“ aktivieren.

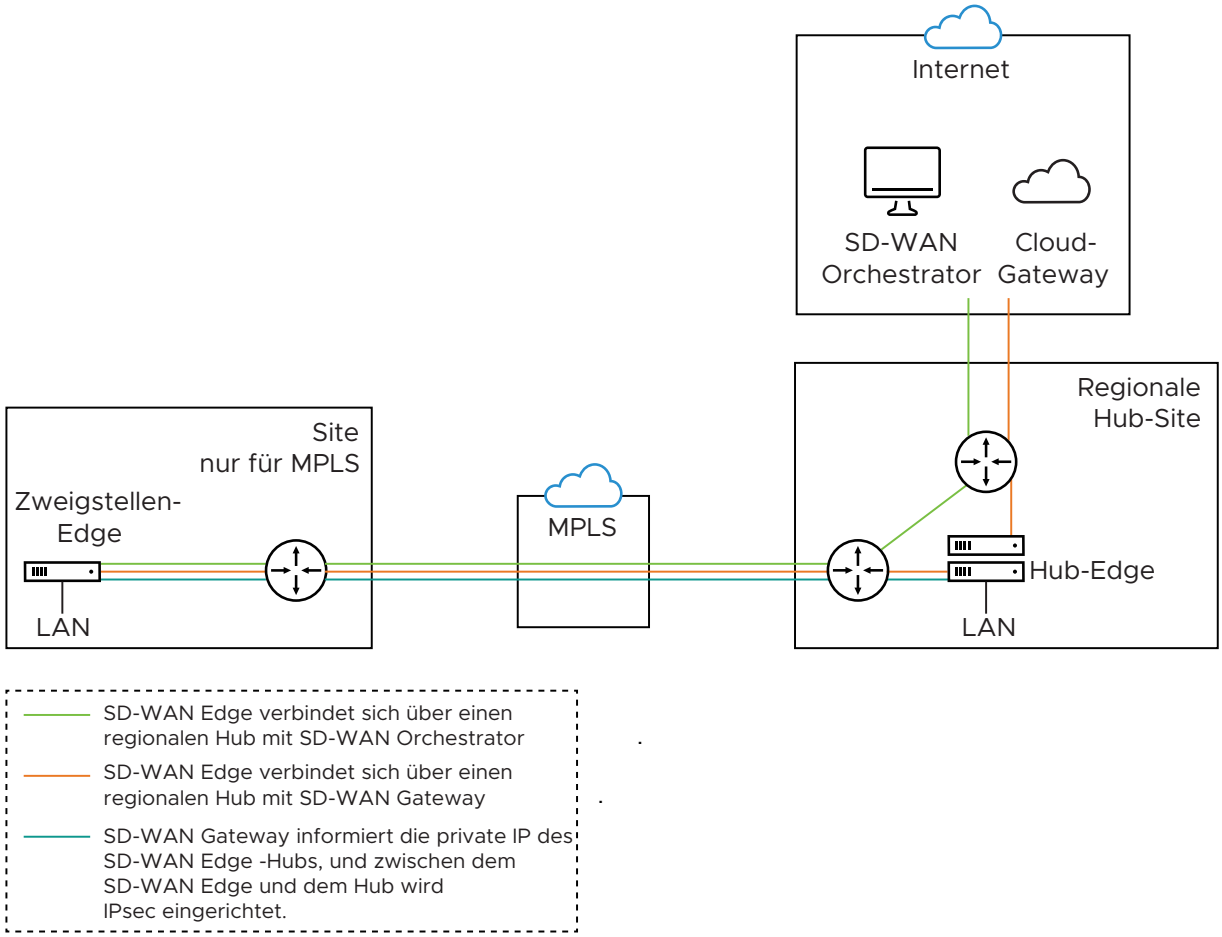
Nur-MPLS-Sites

VMware SD-WAN unterstützt private WAN-Bereitstellungen mit einem gehosteten VMware SD-WAN-Dienst für Kunden mit hybriden Umgebungen, die auf Sites mit nur einem privaten WAN-Link bereitstellen.

In einer Site ohne öffentliche Overlays kann das private WAN als primäres Kommunikationsmittel mit dem VMware SD-WAN-Dienst genutzt werden, einschließlich der folgenden Einstellungen:

- Erreichbarkeit des SD-WAN-Diensts über private Verbindung aktiviert
- NTP-Außerkraftsetzung mithilfe privater NTP-Server aktiviert

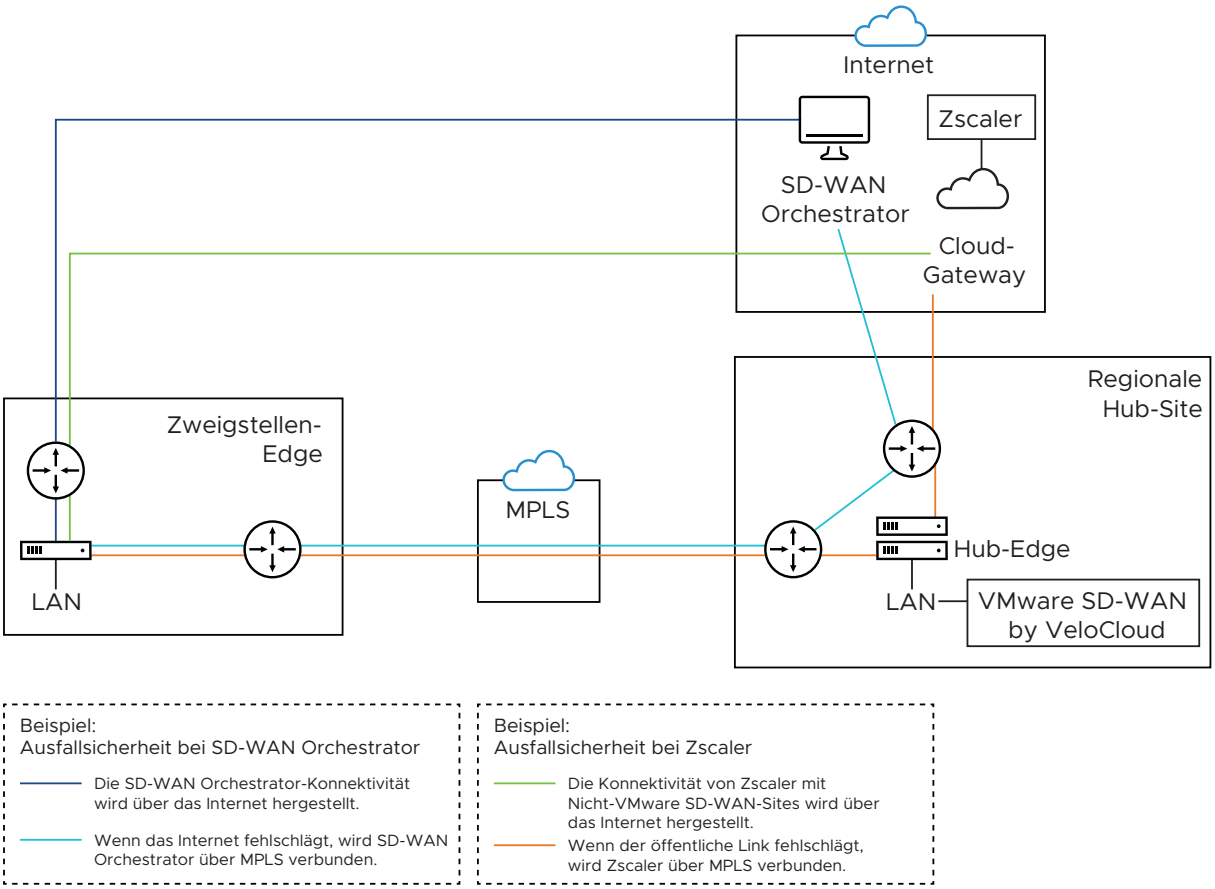
Die folgende Abbildung zeigt einen regionalen Hub mit Internetverbindung und SD-WAN Edge ausschließlich mit MPLS-Verbindung.



Der Datenverkehr vom SD-WAN Edge mit Links vom Typ „Nur MPLS“ wird zum Orchestrator und Gateway über einen regionalen Hub geleitet, der einen Breakout in die Public Cloud durchführen kann. Die Option „SD-WAN-Dienst erreichbar (SD-WAN Service Reachable)“ ermöglicht es dem Edge, online und über den Orchestrator verwaltbar zu bleiben, und lässt eine öffentliche Internetverbindung über das Gateway zu, unabhängig davon, ob es eine öffentliche Link-Konnektivität gibt.

Dynamisches Failover über MPLS

Wenn alle öffentlichen Internetverbindungen ausfallen, können Sie wichtigen Internetdatenverkehr per Failover zu einem privaten WAN-Link verlagern. Die folgende Abbildung veranschaulicht die Resilienz von SD-WAN Orchestrator und Non VMware SD-WAN Site, Zscaler.



- **Orchestrator-Resilienz**: Der Orchestrator stellt eine Verbindung zum Internet her. Wenn das Internet ausfällt, stellt der Orchestrator eine Verbindung über MPLS her. Die Orchestrator-Verbindung wird mithilfe der IP-Adresse eingerichtet, die über MPLS angekündigt wird. Die Verbindung nutzt die öffentliche Internetverbindung im regionalen Hub.
- **Zscaler-Resilienz**: Die Zscaler-Verbindung wird über das Internet eingerichtet. Wenn die öffentliche Verbindung ausfällt, stellt Zscaler die Verbindung über MPLS her.

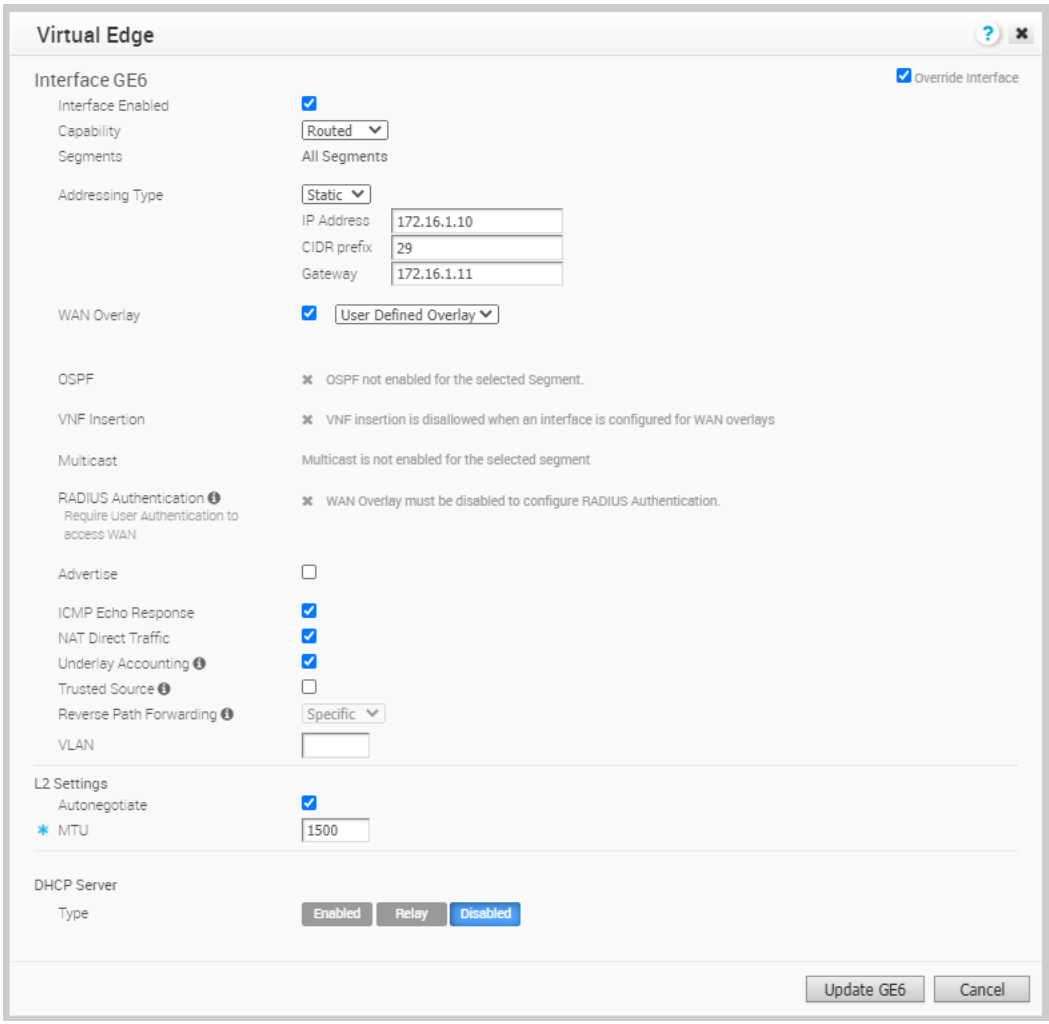
Konfigurieren von „SD-WAN-Dienst erreichbar (SD-WAN Service Reachable)“

1 Klicken Sie im Unternehmensportal auf **Konfigurieren (Configure) > Edges**.

2 Klicken Sie auf der Seite „Edges“ entweder auf das Gerätesymbol neben einem Edge oder klicken Sie auf den Link zu dem Edge und dann auf die Registerkarte **Gerät (Device)**.

3 Scrollen Sie nach unten zu **Schnittstelleneinstellungen (Interface Settings)** und bearbeiten Sie die mit dem MPLS-Link verbundene Schnittstelle über **Bearbeiten (Edit)**.

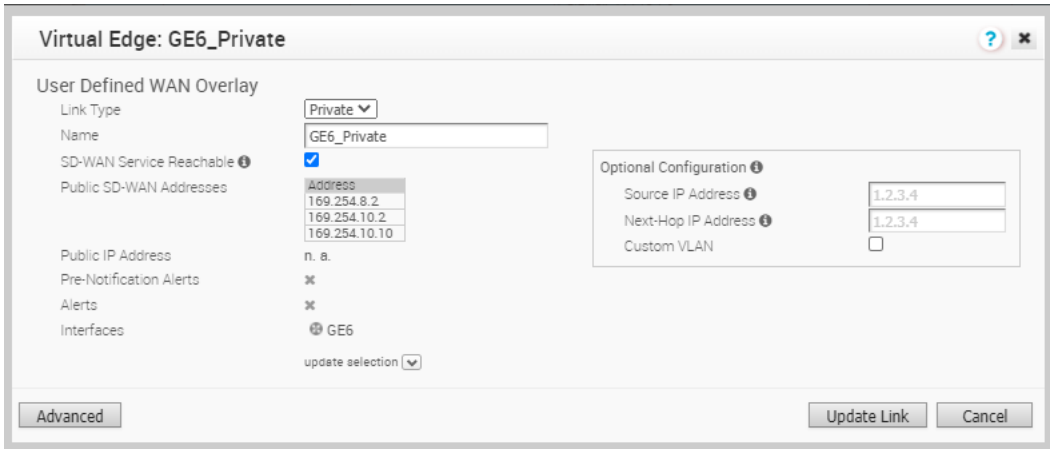
4 Aktivieren Sie im Fenster **Schnittstelle (Interface)** das Kontrollkästchen **Benutzerdefiniertes Overlay (User Defined Overlay)**.



Die Option **SD-WAN-Dienst erreichbar (SD-WAN Service Reachable)** ist nur für ein Netzwerk vom Typ **Benutzerdefiniertes Overlay (User Defined Overlay)** verfügbar.

5 Bearbeiten Sie im Abschnitt **WAN-Einstellungen (WAN Settings)** die mit **Benutzerdefiniertes Overlay (User Defined Overlay)** aktivierte Schnittstelle über die Option **Bearbeiten (Edit)**.

6 Aktivieren Sie im Fenster **Benutzerdefiniertes WAN-Overlay (User Defined WAN Overlay)** das Kontrollkästchen **SD-WAN-Dienst erreichbar (SD-WAN Service Reachable)**, um Sites bereitzustellen, die nur über einen privaten WAN-Link verfügen und/oder die Möglichkeit bieten, ein Failover von kritischem Netzwerkverkehr zu einem privaten WAN-Link durchzuführen.



Wenn Sie das Kontrollkästchen **SD-WAN-Dienst erreichbar (SD-WAN Service Reachable)** aktivieren, wird eine Liste der öffentlichen IP-Adressen von SD-WAN Gateways und SD-WAN Orchestrator angezeigt, die möglicherweise über das private Netzwerk angekündigt werden müssen, wenn noch keine Standardroute über das gleiche private Netzwerk von der Firewall angekündigt wurde.

7 Konfigurieren Sie die übrigen Optionen nach Bedarf und klicken Sie auf **Link aktualisieren (Update Link)**, um die Einstellungen zu speichern.

Weitere Informationen zu den anderen Optionen im Fenster **WAN-Overlay (WAN Overlay)** finden Sie unter Konfigurieren der Einstellungen für Edge-WAN-Overlay.

Konfigurieren von SNMP-Einstellungen auf der Edge-Ebene

SNMP ist ein häufig verwendetes Protokoll für die Netzwerküberwachung, und MIB ist eine Datenbank, die SNMP zur Verwaltung von Entitäten zugeordnet ist. SNMP kann aktiviert werden, indem Sie die gewünschte SNMP-Version auswählen, wie in den Schritten unten erläutert. Auf der Edge-Ebene können Sie die im Profil angegebenen Einstellungen für SNMP außer Kraft setzen, indem Sie das Kontrollkästchen **Edge-Außerkraftsetzung aktivieren (Enable Edge Override)** aktivieren.

Bevor Sie beginnen:

- So laden Sie die SD-WAN Edge-MIB herunter: Navigieren Sie zum Bildschirm **Remote-Diagnose (Remote Diagnostic)** (**Test & Fehlerbehebung > Remote-Diagnose (Test & Troubleshooting > Remote Diagnostics)**) und führen Sie MIB für SD-WAN Edge aus. Kopieren und Einfügen von Ergebnissen auf Ihre lokale Maschine.
- Installieren Sie alle von VELOCLOUD-EDGE-MIB benötigten MIBs auf dem Client-Host, einschließlich SNMPv2-SMI, SNMPv2-CONF, SNMPv2-TC, INET-ADDRESS-MIB, IF-MIB, UUID-TC-MIB und VELOCLOUD-MIB. Alle oben genannten MIBs, außer VELOCLOUD-MIB, können online gefunden werden. Überprüfen Sie für VELOCLOUD-MIB die VeloCloud-Website.

Über diese Aufgabe: Auf der Edge-Ebene können Sie die im Profil angegebenen Einstellungen für SNMP außer Kraft setzen, indem Sie das Kontrollkästchen **Edge-Außerkraftsetzung aktivieren (Enable Edge Override)** aktivieren. Die Option „Edge-Außerkraftsetzung (Edge Override)“ aktiviert Edge-spezifische Änderungen an den angezeigten Einstellungen und deaktiviert weitere automatische Updates aus dem Konfigurationsprofil für dieses Modul. Um die Konsistenz und Benutzerfreundlichkeit zu erleichtern, wird empfohlen, Konfigurationen auf dem Profil statt auf der Edge-Ausnahmeebene festzulegen.

Unterstützte MIBs

- SNMP MIB-2-System
- SNMP MIB-2-Schnittstellen
- VELOCLOUD-EDGE-MIB
- HOST-RESOURCES-MIB, von RFC 1514

Vorgehensweise zum Konfigurieren von SNMP-Einstellungen auf der Edge-Ebene:

1 Rufen Sie VELOCLOUD-EDGE-MIB auf dem Bildschirm „Remote-Diagnose (Remote Diagnostic)“ von SD-WAN Orchestrator ab.

2 Installieren Sie alle MIBs, die von VELOCLOUD-EDGE-MIB benötigt werden.

3 Navigieren Sie in der SD-WAN Orchestrator-Instanz zu **Konfigurieren (Configure) > Edges**.

Der Bildschirm **VeloCloud Edges** wird angezeigt.

4 Wählen Sie einen Edge aus, für den Sie SNMP-Einstellungen konfigurieren möchten, und klicken Sie auf das Symbol **Gerät (Device)** unter der Spalte „Gerät (Device)“.

Der Bildschirm **Konfiguration-Edges (Configuration Edges)** des ausgewählten Edge wird angezeigt.

5 Scrollen Sie nach unten zum Bereich **SNMP-Einstellungen (SNMP Settings)** und aktivieren Sie das Kontrollkästchen **Edge-Außerkraftsetzung aktivieren (Enable Edge Override)**. Sie können zwischen zwei Versionen wählen: v2c oder v3.

6 Führen Sie für eine SNMP v2c-Konfiguration die folgenden Schritte aus:

a Aktivieren Sie das Kontrollkästchen **v2c**.

b Geben Sie einen Port in das Textfeld **Port** ein. Die Standardeinstellung ist 161.

c Geben Sie im Textfeld **Community** ein Wort oder eine Zahlenfolge ein, die als „Kennwort“ fungiert und Ihnen den Zugriff auf den SNMP-Agenten ermöglicht.

d Für zulässige IPs:

- Aktivieren Sie das Kontrollkästchen **Alle (Any)**, damit jede IP-Adresse auf den SNMP-Agenten zugreifen kann.

- Um den Zugriff auf den SNMP-Agenten einzuschränken, deaktivieren Sie das Kontrollkästchen **Alle (Any)** und geben Sie die IP-Adresse(n) ein, die für den Zugriff auf den SNMP-Agenten zulässig ist/sind.

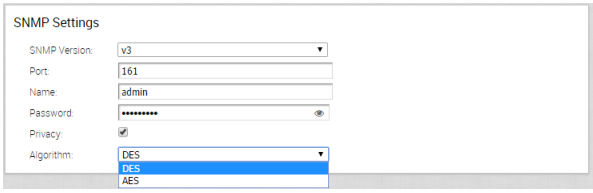
7 Führen Sie für eine SNMP v3-Konfiguration, die zusätzliche Sicherheitsunterstützung bietet, die folgenden Schritte aus:

a Geben Sie einen Port in das Textfeld **Port** ein. Die Standardeinstellung ist 161.

b Geben Sie einen Benutzernamen und ein Kennwort in die entsprechenden Textfelder ein.

c Aktivieren Sie das Kontrollkästchen **Datenschutz (Privacy)**, wenn Sie die Paketübertragung verschlüsseln möchten.

d Wenn Sie das Kontrollkästchen **Datenschutz (Privacy)** aktiviert haben, wählen Sie aus dem Dropdown-Menü **Algorithmus (Algorithm)** „DES“ oder „AES“ aus.



8 Konfigurieren Sie die Firewalleinstellungen. Nachdem Sie SNMP-Einstellungen konfiguriert haben, navigieren Sie zu den Firewalleinstellungen (**Konfigurieren >Profile > Firewall (Configure >Profiles > Firewall)**), um die Firewalleinstellungen zu konfigurieren, die Ihre SNMP-Einstellungen aktivieren.

Hinweis Die Überwachung von SNMP-Schnittstellen wird bei DPDK-aktivierten Schnittstellen nicht unterstützt.

Konfigurieren von Außerkraftsetzungen für WLAN-Funk

Auf der Edge-Ebene können Sie die im Profil angegebenen WLAN-Einstellungen außer Kraft setzen, indem Sie das Kontrollkästchen **Edge-Außerkraftsetzung aktivieren (Enable Edge Override)** aktivieren. Basierend auf dem Edge-Modell und dem für den Edge konfigurierten Land können Sie mit den WLAN-Funkeinstellungen ein für den Edge unterstützten Funkbereich und einen Kanal auswählen.

Führen Sie die folgenden Schritte aus, um die WLAN-Funkeinstellungen auf der Edge-Ebene außer Kraft zu setzen.

Voraussetzungen

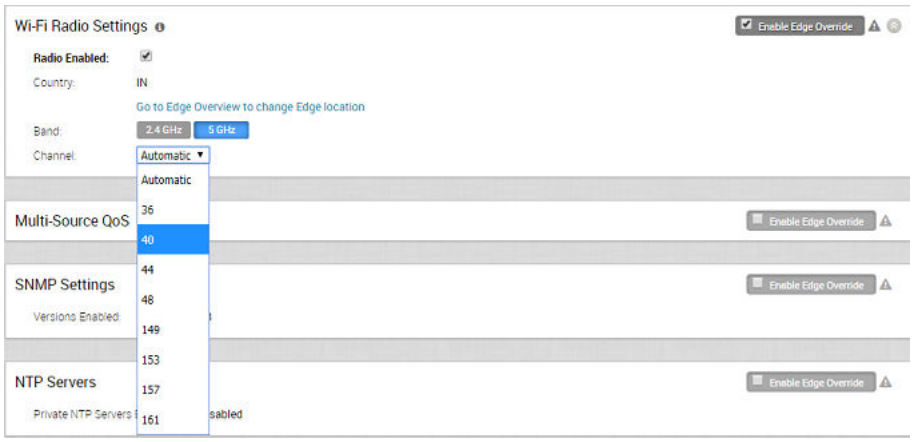
- Bevor Sie den WLAN-Funkbereich und den Kanal für den Edge konfigurieren, ist es wichtig, das richtige Land für den Betrieb des WLAN-Funks einzustellen, um den lokalen Anforderungen für die WLAN-Übertragung zu entsprechen. Stellen Sie sicher, dass das richtige Land für den Edge-Betrieb im Abschnitt **Kontakt und Standort (Contact & Location)** der **Edge-Übersicht (Edge Overview)**-Konfigurationsseite konfiguriert ist. Die Adresse wird automatisch nach dem Aktivieren des Edge eingetragen. Sie können die Adresse jedoch bei Bedarf manuell überschreiben.

  Hinweis Das Land sollte in der 2-Zeichen-Notation nach ISO 3166-1-alpha-2 angegeben werden (z. B. US, DE, IN usw.).

Verfahren

1. Navigieren Sie in der SD-WAN Orchestrator-Instanz zu **Konfigurieren (Configure)** > **Edges**.
2. Wählen Sie einen Edge aus, in dem Sie die WLAN-Funkeinstellungen außer Kraft setzen möchten, und klicken Sie auf das Symbol unter der Spalte **Gerät (Device)**.

   Die Seite **Geräteeinstellung (Device Setting)** für den ausgewählten Edge wird angezeigt.
3. Im Dropdown-Menü **Segment konfigurieren (Configure Segment)** ist standardmäßig die Option **Globales Segment [Normal] (Global Segment [Regular])** ausgewählt. Falls erforderlich, können Sie aus dem Dropdown-Menü ein anderes Profilsegment auswählen.
4. Navigieren Sie zum Bereich **WLAN-Funkeinstellungen (WI-FI Radio Settings)** und aktivieren Sie das Kontrollkästchen **Edge-Außerkraftsetzung aktivieren (Enable Edge Override)**.



5. Wählen Sie unter **Bereich (Band)** einen Funkbereich in den für das Edge unterstützten Funkfrequenzen aus.
6. Wählen Sie im Dropdown-Menü **Kanal (Channel)** einen für den Edge unterstützten Funkkanal aus.

   Hinweis Unter **Bereich (Band)** und **Kanal (Channel)** werden nur die unterstützten Funkbereiche und Kanäle für den konfigurierten Standort des Edge angezeigt.

7 Wenn Sie den Standort des Edge ändern möchten, klicken Sie auf **Zum Ändern des Edge-Standorts zur Edge-Übersicht navigieren (Go to Edge Overview to change edge location)**. Die Seite **Edge-Übersicht (Edge Overview)** wird für den ausgewählten Edge angezeigt.

   a Klicken Sie im Bereich **Kontakt und Standort (Contact & Location)** auf den Link **Standort aktualisieren (Update Location)**, um den Edge-Standort festzulegen, und klicken Sie auf **Änderungen speichern (Save Changes)**.

8 Klicken Sie auf **Änderungen speichern (Save Changes)**. Die WLAN-Funkeinstellungen werden für den ausgewählten Edge außer Kraft gesetzt.

Hinweis Wenn ein Land nicht für den Edge festgelegt ist oder das Land ungültig ist, wird die Funkeinstellung für **Bereich (Band)** auf **2,4 GHz** und die Funkeinstellung für **Kanal (Channel)** auf **Automatisch (Automatic)** festgelegt.

Sicherheits-VNFs

Virtuelle Netzwerkfunktionen (VNFs) sind einzelne Netzwerkdienste, z. B. Router und Firewalls, die als rein softwarebasierte VM-Instanzen auf allgemeiner Hardware ausgeführt werden. Beispielsweise setzt eine Routing-VNF den gesamten Funktionsumfang eines Routers um, wird aber ausschließlich in Form von Software allein oder mit anderen VNFs zusammen auf allgemeiner Hardware ausgeführt. VNFs werden innerhalb der NFV-Architektur verwaltet und orchestriert.

Die Virtualisierung von NFV und VNF bedeutet, dass Netzwerkfunktionen unabhängig von der zugrunde liegenden Hardware in verallgemeinerter Weise umgesetzt werden. VNFs können in jeder beliebigen VM-Umgebung in der Zweigstelle, Cloud oder im Datencenter ausgeführt werden. Mit dieser Architektur haben Sie die folgenden Möglichkeiten:

- Sie können Netzwerkdienste an einem optimalen Speicherort einfügen, um für angemessene Sicherheit zu sorgen. Beispielsweise können Sie eine VNF-Firewall in eine mit dem Internet verbundene Zweigstelle einfügen, anstatt einen (ineffizienten) MPLS-Link zu verwenden, um Datenverkehr durch ein entferntes Datencenter mit Firewallschutz zu fädeln.
- Sie können die Leistung von Anwendungen optimieren. Mithilfe einer VNF für Sicherheit oder für die bevorzugte Behandlung von bestimmtem Datenverkehr kann der Datenverkehr den direktesten Weg zwischen dem Benutzer und der Cloud-Anwendung folgen. In einer VM-Umgebung können mehrere VNFs gleichzeitig ausgeführt werden, voneinander isoliert und unabhängig voneinander geändert oder aktualisiert werden.

In den folgenden Tabellen sind die Firewalls von Drittanbietern aufgeführt, die von VMware SD-WAN unterstützt werden, zusammen mit der Support-Matrix:

Tabelle 16-8. Palo Alto Networks-Firewall – Support-Matrix

VMware SD-WAN Edge-Plattform	Edge 520v	Edge 840	Edge 620	Edge 640	Edge 680
Empfohlene Firewall-Modelle der VM-Serie	VM-50 Lite	VM-100	VM-50 Lite	VM-100	VM-100
Anzahl der verfügbaren vCPUs für die Firewall der VM-Serie	2	2	2	2	2
Verfügbarer Arbeitsspeicher für VNF	4,5 GB	6,5 GB	4,5 GB	6,5 GB	6,5 GB
Verfügbarer Speicherplatz auf Edge für VNF	64 GB	120 GB	64 GB	120 GB	120 GB
VMware SD-WAN-Softwareversion	Version 3.2.0 oder höher	Version 3.2.0 oder höher	Version 3.4.3 oder höher	Version 3.4.3 oder höher	Version 3.4.3 oder höher
Version Panorama	Version 8.0.5 oder höher	Version 8.0.5 oder höher	Version 8.0.5 oder höher	Version 8.0.5 oder höher	Version 8.0.5 oder höher

Tabelle 16-9. Check Point-Firewall – Support-Matrix

VMware SD-WAN Edge-Plattform	Edge 520v	Edge 840	Edge 620	Edge 640	Edge 680
Verfügbarer Arbeitsspeicher für VNF	2 GB	4 GB	2 GB	4 GB	4 GB
Anzahl der verfügbaren vCPUs für VNF	2	2	2	2	2
Verfügbarer Speicher auf Edge für VNF	64 GB	100 GB	120 GB	120 GB	120 GB
Maximaler Durchsatz von SD-WAN und Checkpoint-VNF	100 Mbit/s	550 Mbit/s	100 Mbit/s	350 Mbit/s	500 Mbit/s
VMware SD-WAN-Softwareversion	Version 3.3.2 oder höher	Version 3.3.2 oder höher	Version 3.4.3 oder höher	Version 3.4.3 oder höher	Version 3.4.3 oder höher

Tabelle 16-9. Check Point-Firewall – Support-Matrix (Fortsetzung)

VMware SD-WAN Edge-Plattform	Edge 520v	Edge 840	Edge 620	Edge 640	Edge 680
Version des Checkpoint VNF-Betriebssystems	Version R77.20 oder höher	Version R77.20 oder höher	Version R77.20 oder höher	Version R77.20 oder höher	Version R77.20 oder höher
Version der Checkpoint Manager-Software	Version 80.30 oder höher	Version 80.30 oder höher	Version 80.30 oder höher	Version 80.30 oder höher	Version 80.30 oder höher

Tabelle 16-10. Fortinet-Firewall – Support-Matrix

VMware SD-WAN Edge-Plattform	Edge 520v	Edge 840
Empfohlene Firewall-Modelle der VM-Serie	VM00, VM01	VM00, VM01, VM02
Verfügbarer Arbeitsspeicher für VNF	2 GB	4 GB
Anzahl der verfügbaren vCPUs für VNF	2	2
Verfügbarer Speicher auf Edge für VNF	64 GB	100 GB
Maximaler Durchsatz von SD-WAN und FortiGate VNF	100 Mbit/s	500 Mbit/s
VMware SD-WAN-Softwareversion	Version 3.3.1 oder höher	Version 3.3.1 oder höher
FortiOS-Version	Version 6.0 und 6.2.0	Version 6.0 und 6.2.0

Sie können Datenverkehr über VNF auf einem SD-WAN Edge bereitstellen und weiterleiten.

Konfigurieren des VNF-Verwaltungsdiensts

VMware SD-WAN unterstützt Firewalls von Drittanbietern, die als VNF verwendet werden können, um Datenverkehr durch Edges weiterzuleiten.

Wählen Sie die Firewall eines Drittanbieters aus und konfigurieren Sie die Einstellungen entsprechend. Möglicherweise müssen Sie auch zusätzliche Einstellungen in der Firewall des Drittanbieters konfigurieren. Weitere Konfigurationen finden Sie in den Handbüchern zur Bereitstellung der entsprechenden Drittanbieter-Firewall.

Konfigurieren Sie für die VNF-Typen **Check Point-Firewall** und **Fortinet-Firewall** das VNF-Image mithilfe der Systemeigenschaft **edge.vnf.extraImageInfos**. Für die Konfiguration der Systemeigenschaften benötigen Sie Operator-Benutzerstatus. Wenn Sie keinen Zugriff auf die Operator-Rolle haben, wenden Sie sich für die Konfiguration des VNF-Image an Ihren Operator.

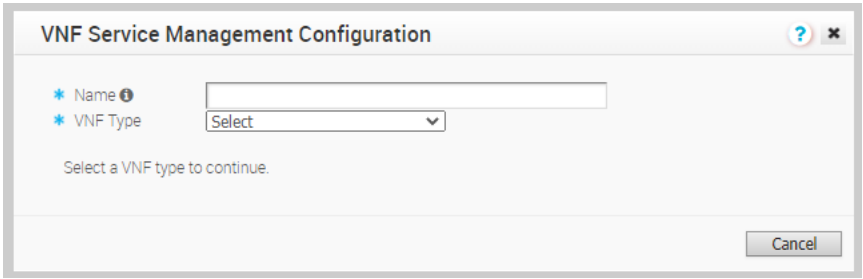
Hinweis In der Systemeigenschaft müssen Sie den korrekten Prüfsummenwert angeben. Der Edge berechnet die Prüfsumme des heruntergeladenen VNF-Image und vergleicht den Wert mit dem in der Systemeigenschaft verfügbaren Wert. Der Edge stellt die VNF nur bereit, wenn beide Prüfsummenwerte gleich sind.

Verfahren

1 Klicken Sie im Unternehmensportal auf **Konfigurieren (Configure) > Netzwerkdienste (Network Services)**.

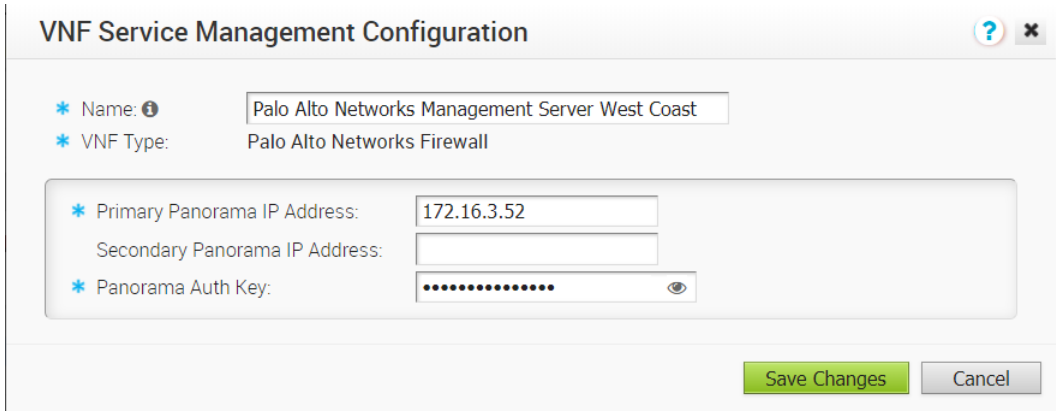
2 Scrollen Sie auf der Seite **Dienste (Services)** nach unten zum Abschnitt **VNFs** und klicken Sie auf **Neu (New)**.

3 Geben Sie im Fenster **Konfiguration des VNF-Verwaltungsdiensts (VNF Service Management Configuration)** einen beschreibenden Namen für den Sicherheits-VNF-Dienst ein und wählen Sie einen VNF-Typ aus der Dropdown-Liste aus.



4 Konfigurieren Sie die Einstellungen basierend auf dem ausgewählten VNF-Typ.

a Konfigurieren Sie für den VNF-Typ **Palo Alto Networks-Firewall (Palo Alto Networks Firewall)** Folgendes:



1 **Primäre Panorama-IP-Adresse (Primary Panorama IP Address)** – Geben Sie die primäre IP-Adresse des Panorama-Servers ein.

2 **Sekundäre Panorama-IP-Adresse (Primary Panorama IP Address)** – Geben Sie die sekundäre IP-Adresse des Panorama-Servers ein.

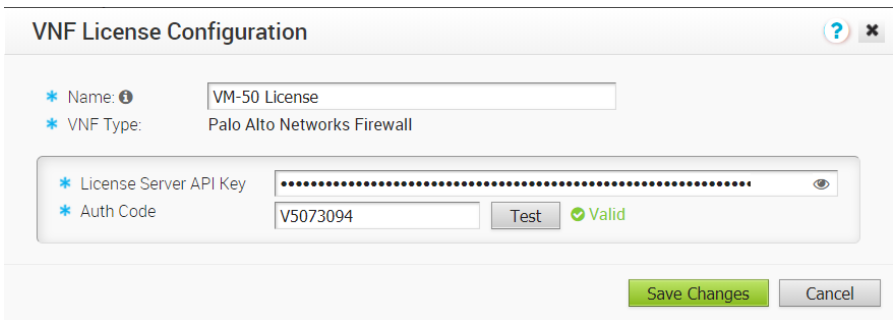
3 **Panorama-Authentifizierungsschlüssel (Panorama Auth Key)** – Geben Sie den auf dem Panorama-Server konfigurierten Authentifizierungsschlüssel ein. VNF verwendet den Authentifizierungsschlüssel, um sich bei Panorama anzumelden und zu kommunizieren.

4 Klicken Sie auf **Änderungen speichern (Save Changes)**.

Definieren Sie nach der Konfiguration von Palo Alto Networks als VNF-Typ die VNF-Lizenzen. Diese Lizenzen werden auf einen oder mehrere VNF-konfigurierte Edges angewendet.

1 Scrollen Sie auf der Seite **Dienste (Services)** nach unten zum Abschnitt **VNF-Lizenzen (VNF Licenses)** und klicken Sie auf **Neu (New)**.

2 Konfigurieren Sie im Fenster **Konfiguration der VNF-Lizenzen (VNF License Configuration)** die folgenden Einstellungen:



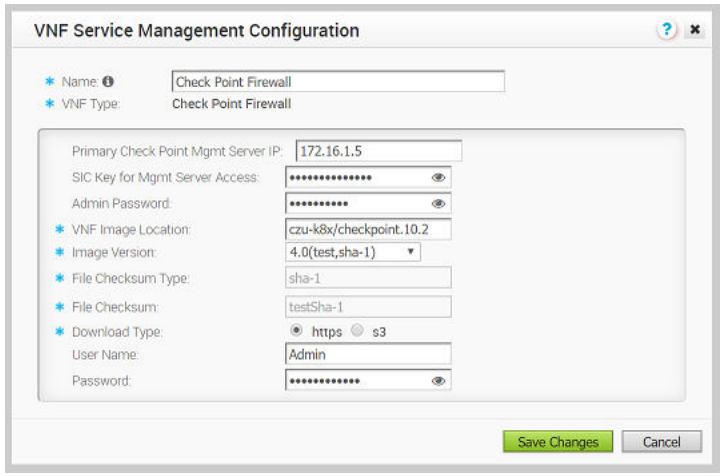
- **Name** – Geben Sie einen beschreibenden Namen für die VNF-Lizenz ein.

- **VNF-Typ (VNF Type)** – Wählen Sie den VNF-Typ aus der Dropdown-Liste aus. Derzeit ist **Palo Alto Networks-Firewall (Palo Alto Networks Firewall)** die einzige verfügbare Option.
- **Lizenzserver-API-Schlüssel (License Server API Key)** – Geben Sie den Lizenzschlüssel aus Ihrem Palo Alto Networks-Konto ein. SD-WAN Orchestrator verwendet diesen Schlüssel zur Kommunikation mit dem Palo Alto Networks-Lizenzserver.
- **Autorisierungscode (Auth Code)** – Geben Sie den von Palo Alto Networks gekauften Autorisierungscode ein.
- Klicken Sie auf **Test (Testen)**, um die Konfiguration zu prüfen.

3 Klicken Sie auf **Änderungen speichern (Save Changes)**.

Sie können die VNF-Lizenzen beim Konfigurieren der **Palo Alto Networks-Firewall (Palo Alto Networks Firewall)** als VNF-Typ auf Edges anwenden.

b Konfigurieren Sie für den VNF-Typ **Check Point-Firewall (Check Point Firewall)** die folgenden Einstellungen:



1 **Primäre IP für den Check Point-Verwaltungsserver (Primary Check Point Mgmt Server IP)** – Geben Sie die IP-Adresse der Check Point-Smart-Konsole ein, die eine Verbindung zur Check Point-Firewall herstellt.

2 **SIC-Schlüssel für den Zugriff auf den Verwaltungsserver (SIC Key for Mgmt Server Access)** – Geben Sie das Kennwort ein, mit dem die VNF in der Check Point-Smart-Konsole registriert wird.

3 **Administratorkennwort (Admin Password)** – Geben Sie das Administratorkennwort ein.

4 **VNF-Image-Speicherort (VNF Image Location)** – Geben Sie den Image-Speicherort ein, von dem der SD-WAN Orchestrator das VNF-Image herunterladen soll.

5 **Image-Version (Image Version)** – Wählen Sie eine Version des VNF-Image für Check Point aus der Dropdown-Liste aus. Die Image-Version wird von der Systemeigenschaft **edge.vnf.extraImageInfos** abgeleitet.

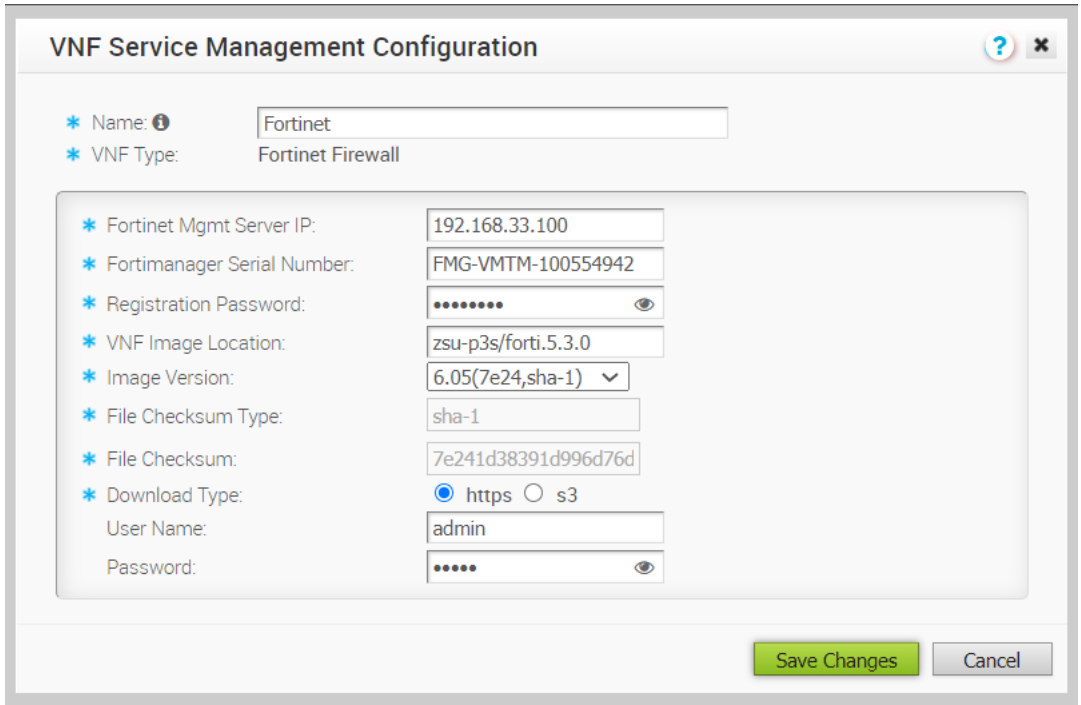
6 **Dateiprüfsummentyp (File Checksum Type)** – Gibt die Methode zur Validierung des VNF-Image an und wird automatisch ausgefüllt, nachdem Sie eine Image-Version ausgewählt haben.

7 **Dateiprüfsumme (File Checksum)** – Gibt die Prüfsumme zur Validierung des VNF-Image an und wird automatisch ausgefüllt, nachdem Sie eine Image-Version ausgewählt haben. Der Prüfsummenwert wird von der Systemeigenschaft **edge.vnf.extraImageInfos** abgeleitet.

8 **Download-Typ (Download Type)** – Wählen Sie den Image-Typ aus. Geben Sie für **https** Ihren Benutzernamen und Ihr Kennwort ein. Geben Sie für **s3** die Parameter AccessKeyid und SecretAccessKey ein.

9 Klicken Sie auf **Änderungen speichern (Save Changes)**.

c Konfigurieren Sie für den VNF-Typ **Fortinet-Firewall (Fortinet Firewall)** die folgenden Einstellungen:



1 **IP des Fortinet-Verwaltungsservers (Fortinet Mgmt Server IP)** – Geben Sie die IP-Adresse des FortiManagers ein, um eine Verbindung zum FortiGate herzustellen.

2 **Seriennummer von FortiManager (Fortimanager Serial Number)** – Geben Sie die Seriennummer von FortiManager ein.

3 **Registrierungskennwort (Registration Password)** – Geben Sie das Kennwort für die Registrierung der VNF beim FortiManager ein.

4 **VNF-Image-Speicherort (VNF Image Location)** – Geben Sie den Image-Speicherort ein, von dem der SD-WAN Orchestrator das VNF-Image herunterladen soll.

5 **Image-Version (Image Version)** – Wählen Sie eine Version des VNF-Image für Fortinet aus der Dropdown-Liste aus. Die folgenden Optionen stehen zur Verfügung: 6.05 und 6.20. Die Image-Version wird von der Systemeigenschaft **edge.vnf.extraImageInfos** abgeleitet.

6 **Dateiprüfsummentyp (File Checksum Type)** – Gibt die Methode zur Validierung des VNF-Image an und wird automatisch ausgefüllt, nachdem Sie eine Image-Version ausgewählt haben.

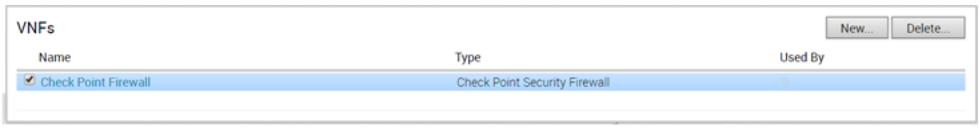
7 **Dateiprüfsumme (File Checksum)** – Gibt die Prüfsumme zur Validierung des VNF-Image an und wird automatisch ausgefüllt, nachdem Sie eine Image-Version ausgewählt haben. Der Prüfsummenwert wird von der Systemeigenschaft **edge.vnf.extraImageInfos** abgeleitet.

8 **Download-Typ (Download Type)** – Wählen Sie den Image-Typ aus. Geben Sie für **https** Ihren Benutzernamen und Ihr Kennwort ein. Für **s3**, AccessKeyid und SecretAccessKey.

9 Klicken Sie auf **Änderungen speichern (Save Changes)**.

Ergebnisse

Im Abschnitt **VNFs** werden die erstellten VNF-Dienste angezeigt. Die folgende Abbildung zeigt ein Beispiel für den VNF-Typ Check Point-Firewall.



Nächste Schritte

Sie können Sicherheits-VNF für einen Edge konfigurieren, um den Datenverkehr über die VNF-Verwaltungsdienste zu leiten. Weitere Informationen finden Sie unter Konfigurieren von Sicherheits-VNF.

Konfigurieren von Sicherheits-VNF

Sie können Datenverkehr über VNF auf dem SD-WAN Edge bereitstellen und weiterleiten, indem Sie Firewalls von Drittanbietern verwenden.

Nur ein Operator kann die Konfiguration der Sicherheits-VNF aktivieren. Falls die Option „Sicherheits-VNF (Security VNF)“ für Sie nicht verfügbar ist, wenden Sie sich an Ihren Operator.

Voraussetzungen

Sie benötigen Folgendes:

- SD-WAN Orchestrator und aktivierten SD-WAN Edge mit laufenden Softwareversionen, die die Bereitstellung einer bestimmten Sicherheits-VNF unterstützen. Weitere Informationen zu den unterstützten Softwareversionen und Edge-Plattformen finden Sie in der Support-Matrix in Sicherheits-VNFs.
- VNF-Manager-Add-on-Lizenz.
- Konfigurierten VNF-Verwaltungsdienst. Weitere Informationen finden Sie unter Konfigurieren des VNF-Verwaltungsdiensts.

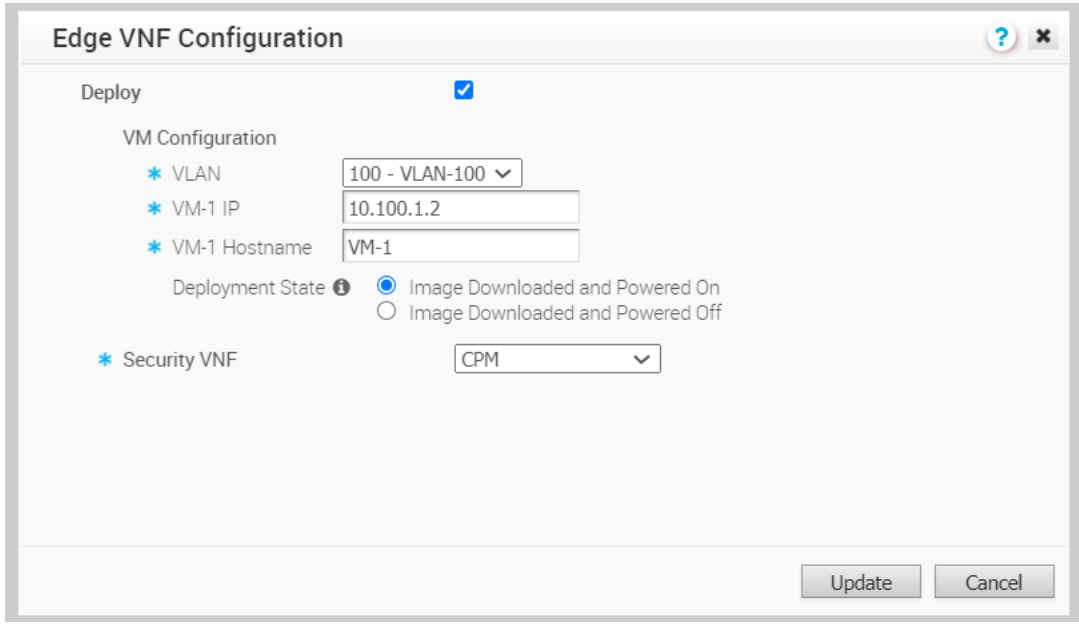
Verfahren

1. Klicken Sie im Unternehmensportal auf **Konfigurieren (Configure) > Edges**.
2. Klicken Sie auf der Seite **Edges** entweder auf das **Gerätesymbol** neben einem Edge oder klicken Sie auf den Link zu einem Edge und dann auf die Registerkarte **Gerät (Device)**.
3. Scrollen Sie auf der Seite **Gerät (Device)** nach unten zum Abschnitt **Sicherheits-VNF (Security VNF)** und klicken Sie auf **Bearbeiten (Edit)**.

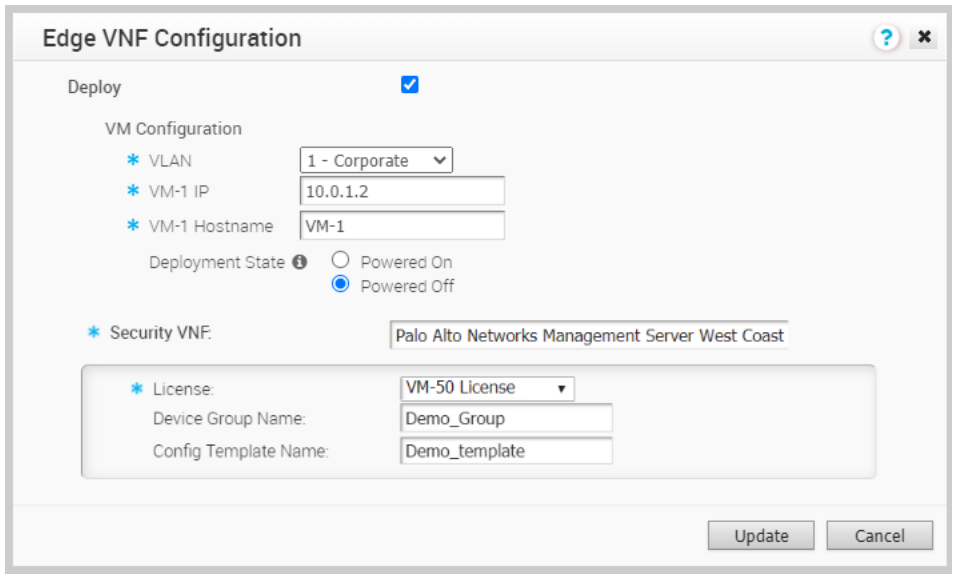
4. Aktivieren Sie im Fenster **Edge-VNF-Konfiguration (Edge VNF Configuration)** das Kontrollkästchen **Bereitstellen (Deploy)**.
5. Konfigurieren Sie die folgenden Einstellungen in der **VM-Konfiguration (VM Configuration)**:
   a. **VLAN** – Wählen Sie aus der Dropdown-Liste ein VLAN aus, das für die VNF-Verwaltung verwendet werden soll.
   b. **IP-Adresse für VM-1 (VM-1 IP)** – Geben Sie die IP-Adresse der VM ein und stellen Sie sicher, dass sich die IP-Adresse im Subnetzbereich des ausgewählten VLAN befindet.
   c. **Hostname für VM-1 (VM-1 Hostname)** – Geben Sie einen Namen für den VM-Host ein.
   d. **Bereitstellungszustand (Deployment State)** – Wählen Sie eine der folgenden Optionen aus:
      - **Image heruntergeladen und eingeschaltet (Image Downloaded and Powered On)** – Diese Option aktiviert die VM, nachdem die Firewall-VNF auf dem Edge erstellt wurde. Der Datenverkehr durchläuft die VNF nur, wenn diese Option ausgewählt ist. Dazu muss mindestens ein VLAN oder eine geroutete Schnittstelle für die VNF-Einfügung konfiguriert sein.
      - **Image heruntergeladen und ausgeschaltet (Image Downloaded and Powered Off)** – Bei dieser Option bleibt die VM ausgeschaltet, nachdem die Firewall-VNF auf dem Edge erstellt wurde. Wählen Sie diese Option nicht aus, wenn Sie den Datenverkehr über die VNF senden möchten.

e **Sicherheits-VNF (Security VNF)** – Wählen Sie einen vordefinierten VNF-Verwaltungsdienst aus der Dropdown-Liste aus. Sie können auch auf **Neuer VNF-Dienst (New VNF Service)** klicken, um einen neuen VNF-Verwaltungsdienst zu erstellen. Weitere Informationen finden Sie unter Konfigurieren des VNF-Verwaltungsdiensts.

Die folgende Abbildung zeigt ein Beispiel für die **Check Point-Firewall** als Sicherheits-VNF-Typ.



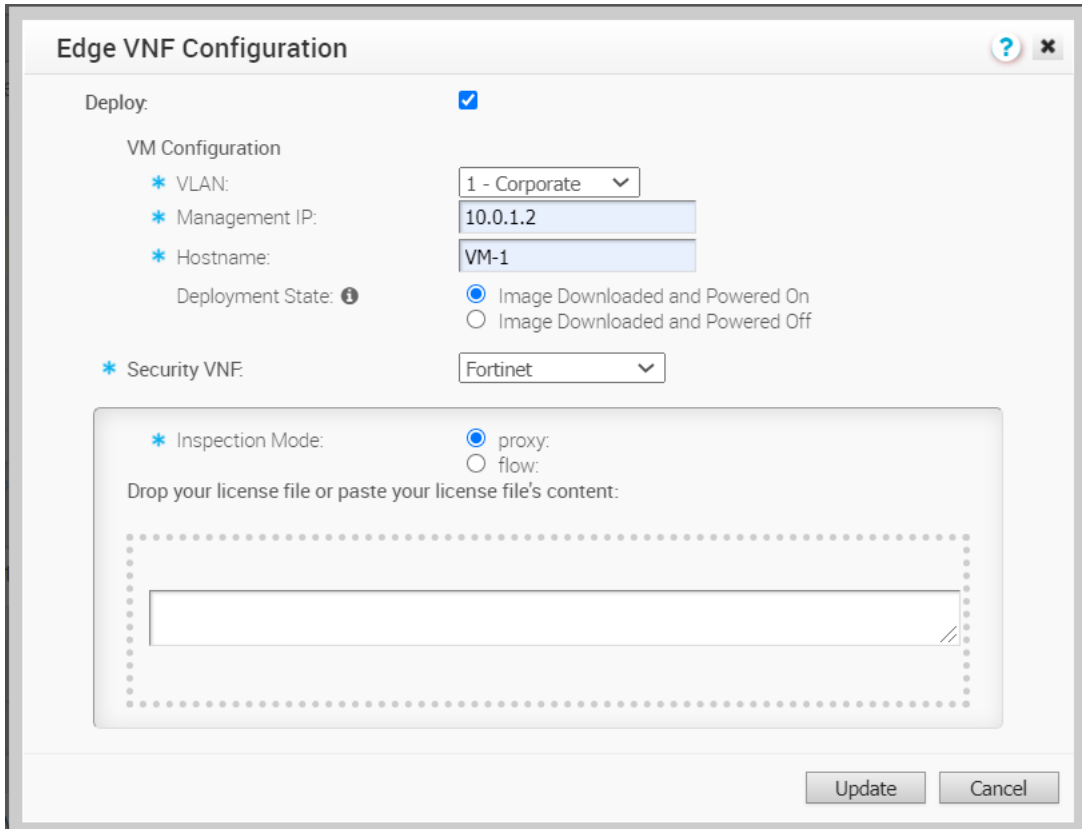
Konfigurieren Sie die folgenden zusätzlichen Einstellungen, wenn Sie **Palo Alto Networks-Firewall (Palo Alto Networks Firewall)** als Sicherheits-VNF wählen:



- **License (Lizenz)** – Wählen Sie die VNF-Lizenz aus der Dropdown-Liste aus.
- **Gerätegruppenname (Device Group Name)** – Geben Sie den auf dem Panorama-Server vorkonfigurierten Gerätegruppennamen ein.

- **Name der Konfigurationsvorlage (Config Template Name)** – Geben Sie den auf dem Panorama-Server vorkonfigurierten Namen der Konfigurationsvorlage ein.

Konfigurieren Sie die folgenden zusätzlichen Einstellungen, wenn Sie **Fortinet-Firewall (Fortinet Firewall)** wählen:



- **Überprüfungsmodus (Inspection Mode)** – Wählen Sie einen der folgenden Modi aus:
  - **Proxy** – Diese Option ist standardmäßig ausgewählt. Die Proxy-basierte Überprüfung beinhaltet die Pufferung des Datenverkehrs und die Untersuchung der Daten als Ganzes zur Analyse.
  - **Flow** – Die Flow-basierte Überprüfung untersucht die Datenverkehrsdaten, während sie ohne Pufferung durch die FortiGate-Einheit geleitet werden.
- **Lizenz (License)** – Dient zum Ziehen und Ablegen der VM-Lizenz.

f Klicken Sie auf **Aktualisieren (Update)**.

Ergebnisse

Die Konfigurationsdetails werden im Abschnitt **Sicherheits-VNF (Security VNF)** angezeigt.

Nächste Schritte

Wenn Sie mehrere Datenverkehrssegmente zur VNF umleiten möchten, definieren Sie die Zuordnung zwischen Segmenten und Dienst-VLANs. Weitere Informationen finden Sie unter Definieren von Zuordnungssegmenten mit Dienst-VLANs.

Sie können die Sicherheits-VNF sowohl in ein VLAN als auch in eine geroutete Schnittstelle einfügen, um den Datenverkehr vom VLAN oder der gerouteten Schnittstelle zur VNF umzuleiten. Weitere Informationen finden Sie unter Konfigurieren von VLAN mit VNF-Einfügung.

Definieren von Zuordnungssegmenten mit Dienst-VLANs

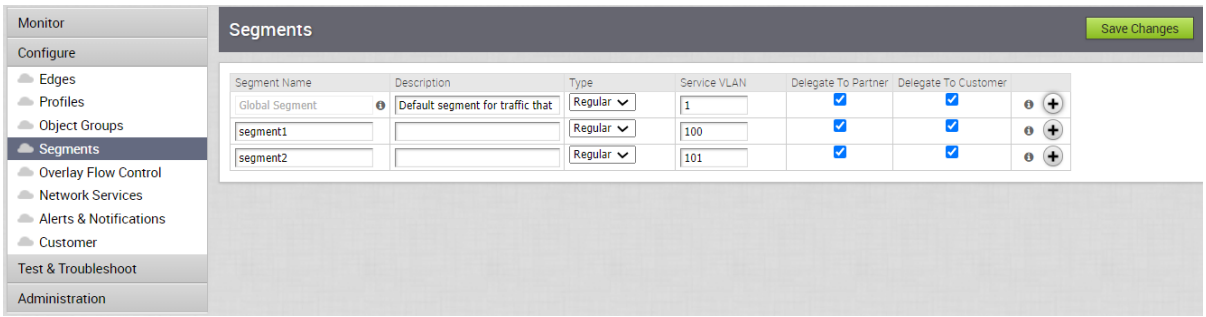
Wenn Sie mehrere Datenverkehrssegmente zur Sicherheits-VNF umleiten möchten, definieren Sie die Zuordnung zwischen Segmenten und Dienst-VLANs.

So ordnen Sie die Segmente mit den Dienst-VLANs zu:

Verfahren

1 Klicken Sie im Unternehmensportal auf **Konfigurieren (Configure) > Segmente (Segments)**.

2 Geben Sie auf der Seite **Segmente (Segments)** die Dienst-VLAN-ID für jedes Segment ein.



3 Klicken Sie auf **Änderungen speichern (Save Changes)**.

Ergebnisse

Dem Segment, in das die VNF eingefügt wird, wird eine eindeutige VLAN-ID zugewiesen. Anhand dieser VLAN-IDs wird die Firewallrichtlinie auf der VNF definiert. Der Datenverkehr von VLANs und Schnittstellen innerhalb dieser Segmente wird mit der für das angegebene Segment zugewiesenen VLAN-ID markiert.

Nächste Schritte

Fügen Sie die Sicherheits-VNF in ein Dienst-VLAN oder eine geroutete Schnittstelle ein, um den Datenverkehr vom VLAN oder der gerouteten Schnittstelle zur VNF umzuleiten. Weitere Informationen finden Sie unter Konfigurieren von VLAN mit VNF-Einfügung.

Konfigurieren von VLAN mit VNF-Einfügung

Sie können die Sicherheits-VNF sowohl in das VLAN als auch in die geroutete Schnittstelle einfügen.

Voraussetzungen

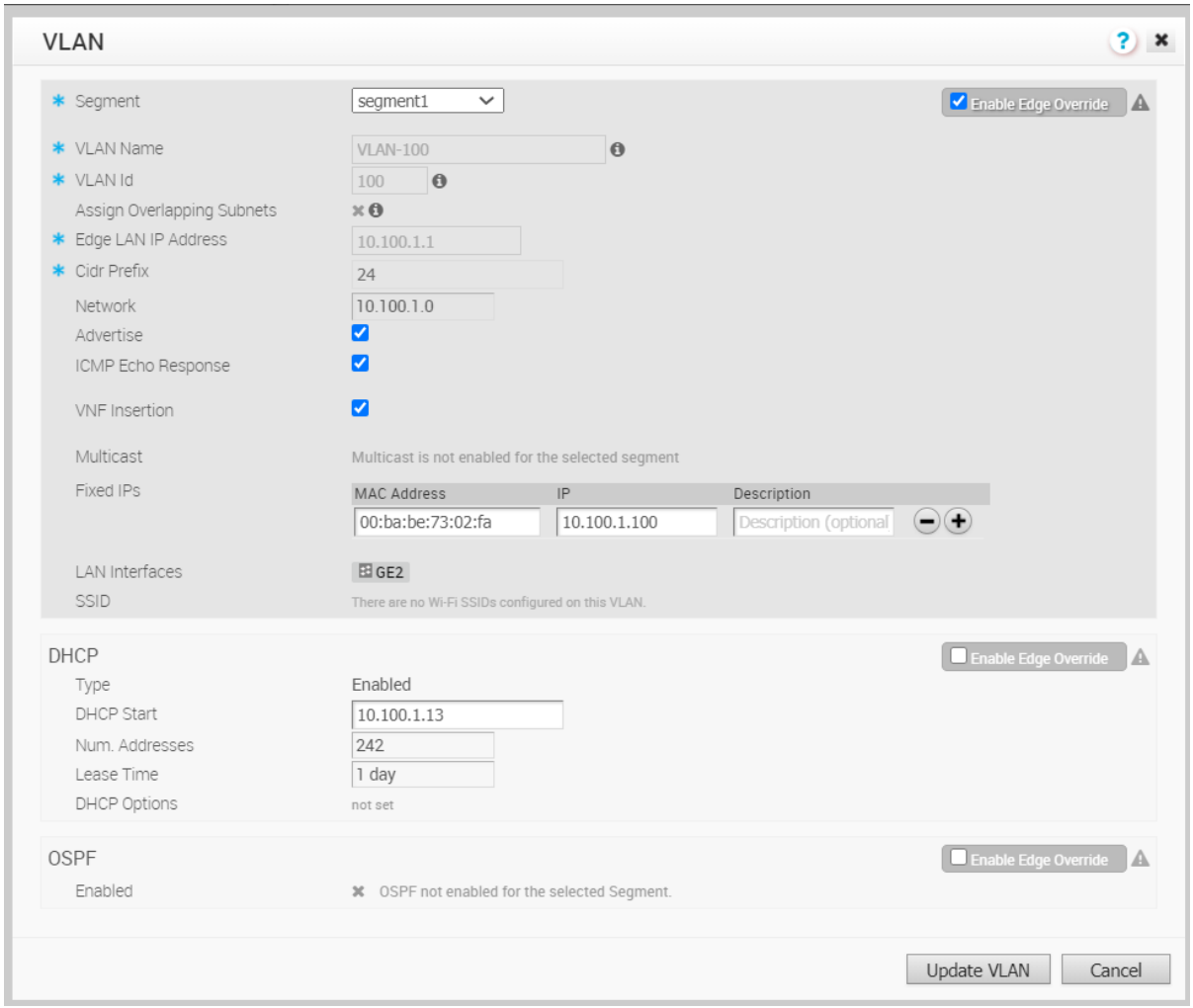
Sie müssen eine Sicherheits-VNF erstellt und die Einstellungen konfiguriert haben. Weitere Informationen finden Sie unter Konfigurieren von Sicherheits-VNF.

Ordnen Sie die Segmente mit Dienst-VLANs zu, um das Einfügen der VNF in die VLANs zu ermöglichen. Weitere Informationen finden Sie unter Definieren von Zuordnungssegmenten mit Dienst-VLANs.

Verfahren

1. Klicken Sie im Unternehmensportal auf **Konfigurieren (Configure) > Edges**.
2. Klicken Sie auf der Seite **Edges** entweder auf das **Gerätesymbol** neben einem Edge oder klicken Sie auf den Link zu einem Edge und dann auf die Registerkarte **Gerät (Device)**.
3. Scrollen Sie auf der Registerkarte **Gerät (Device)** nach unten zum Abschnitt **VLAN konfigurieren (Configure VLAN)**.
4. Klicken Sie auf den Link **Bearbeiten (Edit)** des VLAN, in das die VNF eingefügt werden soll.

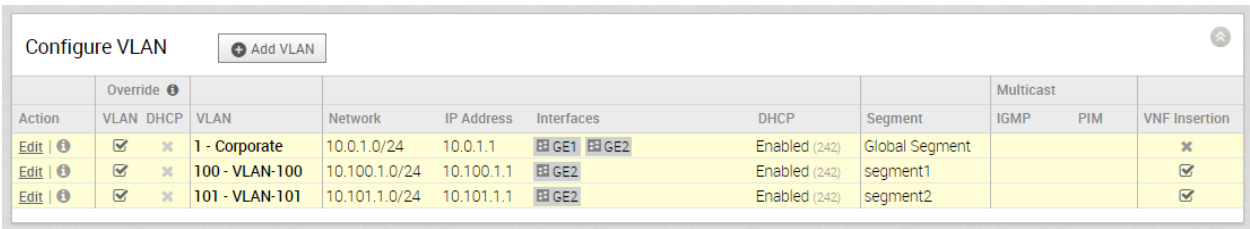
5 Aktivieren Sie im Fenster **VLAN** das Kontrollkästchen **VNF-Einfügung (VNF Insertion)**, um die VNF in das VLAN einzufügen. Mit dieser Option wird der Datenverkehr von einem bestimmten VLAN zur VNF umgeleitet.



6 Klicken Sie auf **VLAN aktualisieren (Update VLAN)**.

Ergebnisse

Im Abschnitt **VLAN konfigurieren (Configure VLAN)** wird der Status der VNF-Einfügung angezeigt.



Sie können die VNF auch in Layer-3-Schnittstellen oder -Teilschnittstellen einfügen. Mit dieser Einfügung wird der Datenverkehr von den Layer-3-Schnittstellen bzw. -Teilschnittstellen zur VNF umgeleitet.

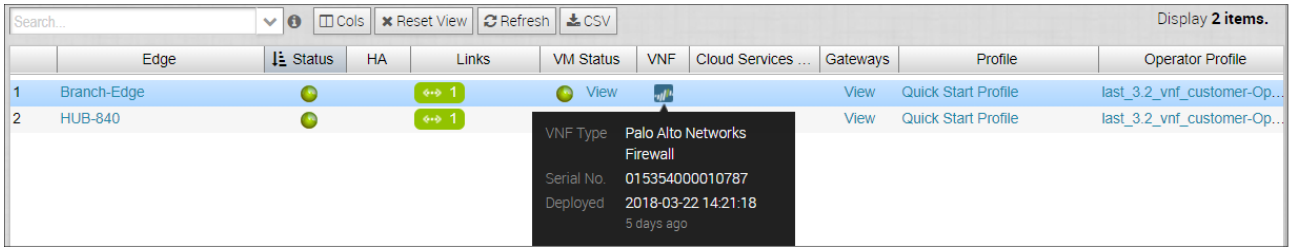
Wenn Sie die geroutete Schnittstelle verwenden, müssen Sie darauf achten, dass die vertrauenswürdige Quelle aktiviert und das WAN-Overlay auf dieser Schnittstelle deaktiviert ist.

Überwachen von VNF für einen Edge

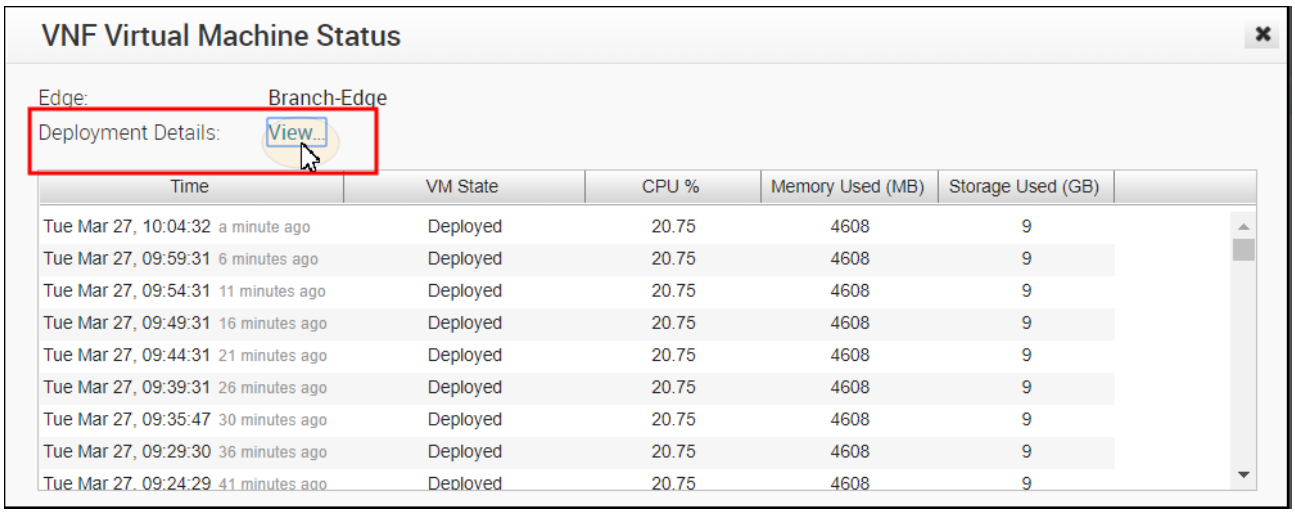
Sie können den Status von VNFs und VMs für einen Edge überwachen und auch die für das Unternehmen konfigurierten VNF-Netzwerkdienste anzeigen.

So überwachen Sie den Status von VNFs und VMs eines Edge:

- Klicken Sie im Unternehmensportal auf **Überwachen (Monitor) > Edges**. Die Liste der Edges wird zusammen mit den Details der konfigurierten VNFs angezeigt.

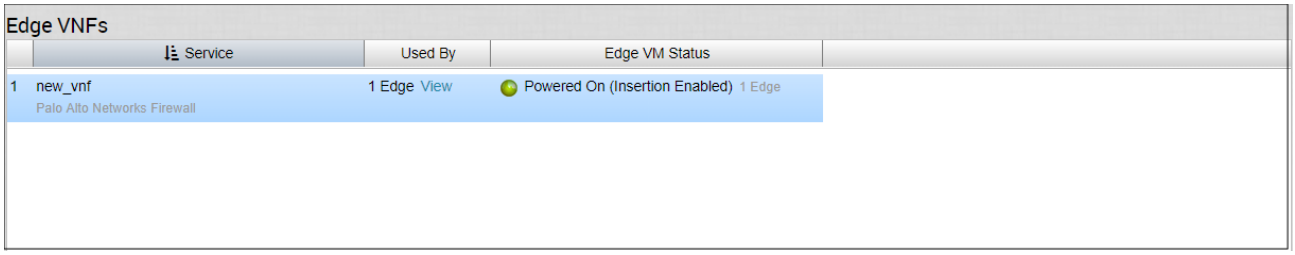


- Bewegen Sie den Mauszeiger über das Symbol in der Spalte **VNF**, um weitere Details des VNF-Typs anzuzeigen.
- Klicken Sie in der Spalte **VM-Status (VM Status)** auf den Link **Anzeigen (View)**, um das Fenster **VNF-VM-Status (VNF Virtual Machine Status)** zu öffnen, wo Sie sich den Bereitstellungsstatus für den Edge ansehen können. Klicken Sie zum Anzeigen der Bereitstellungsdetails neben **Bereitstellungsdetails (Deployment Details)** auf den Link **Anzeigen (View)**.



So überwachen Sie den Status von VNFs und VMs:

- Klicken Sie im Unternehmensportal auf **Überwachen (Monitor) > Netzwerkdienste (Network Services)**. Die Liste der Edges wird zusammen mit den Details der konfigurierten VNFs angezeigt.



VNF-Ereignisse

Sie können die Ereignisse anzeigen, wenn die VNF-VM bereitgestellt wird, wenn sich die VNF-VM-Konfiguration ändert und wenn eine VNF-Einfügung in einem VLAN aktiviert wird.

Klicken Sie im Unternehmensportal auf **Überwachen (Monitor) > Ereignisse (Events)**.

Um die Ereignisse im Zusammenhang mit VNF anzuzeigen, können Sie die Filteroption verwenden. Klicken Sie auf den Dropdown-Pfeil neben der Option **Search (Search)** und wählen Sie aus, ob nach der Spalte „Ereignis (Event)“ oder der Spalte „Meldung (Message)“ gefiltert werden soll.

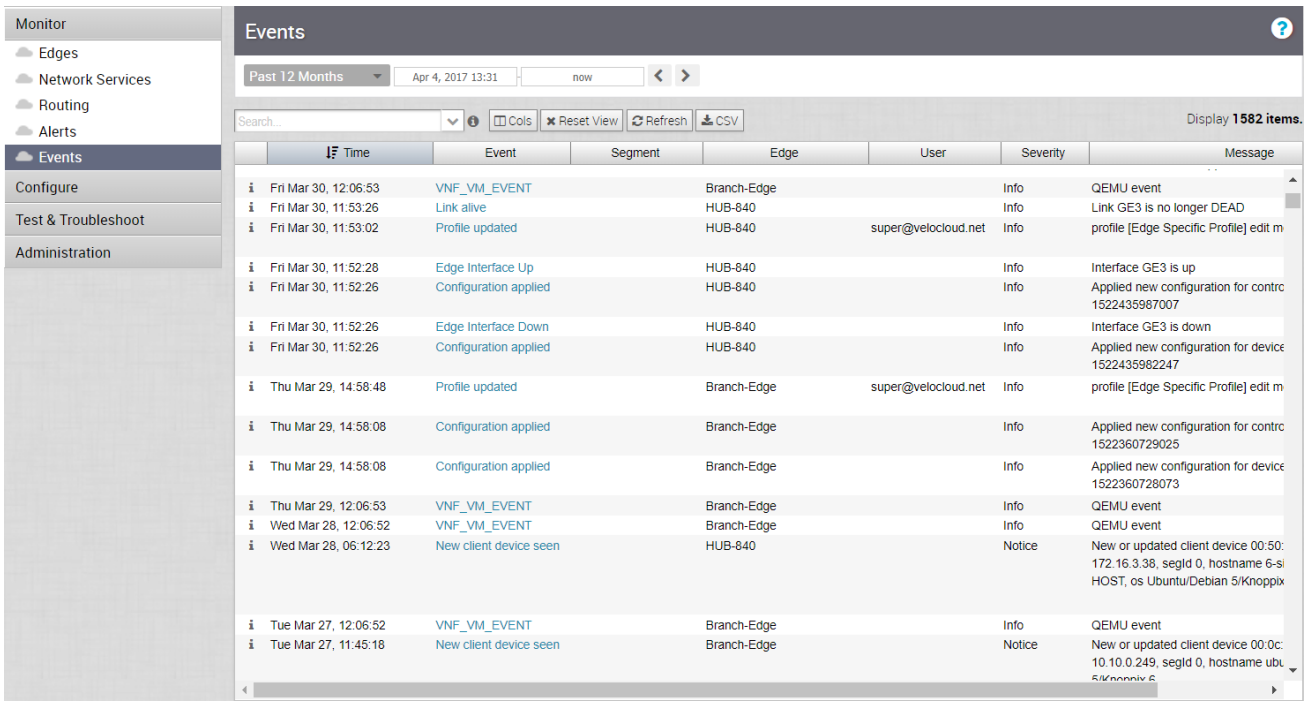
Die folgenden Ereignisse treten ein, wenn sich die Konfiguration von VNF ändert:

- VNF-VM-Konfiguration wurde geändert
- VNF-VM gelöscht
- VNF-VM bereitgestellt
- VNF-VM-Fehler
- VNF-Image-Download-Ereignis

Die folgenden Ereignisse treten ein, wenn die VNF-Einfügung in einem VLAN oder einer gerouteten Schnittstelle aktiviert oder deaktiviert wird.

- VNF-Einfügung deaktiviert
- VNF-Einfügung aktiviert

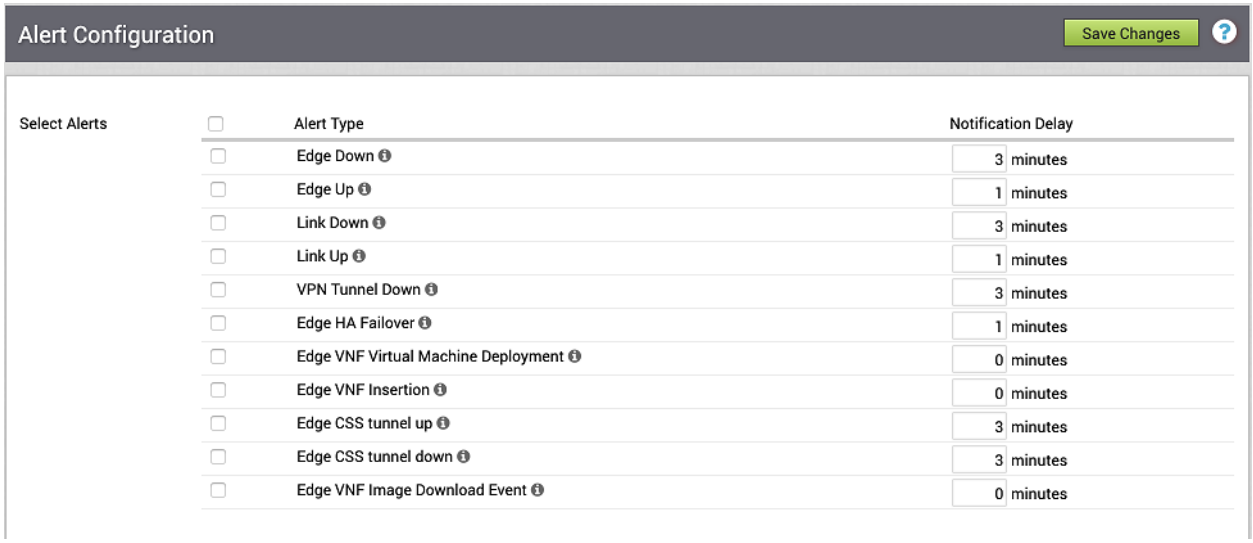
In der folgenden Abbildung sind einige der VNF-Ereignisse dargestellt.



Konfigurieren von VNF-Warnungen

Sie können festlegen, dass Sie Warnungen und Benachrichtigungen im Zusammenhang mit den VNF-Ereignissen erhalten.

Klicken Sie im Unternehmensportal auf **Konfigurieren (Configure) > Warnungen und Benachrichtigungen (Alerts & Notifications)**. Auf der Seite **Warnungskonfiguration (Alert Configuration)** können Sie die Alarmtypen auswählen.



Um Warnungen für VNF-Ereignisse zu erhalten, wählen Sie die folgenden Warnungstypen aus:

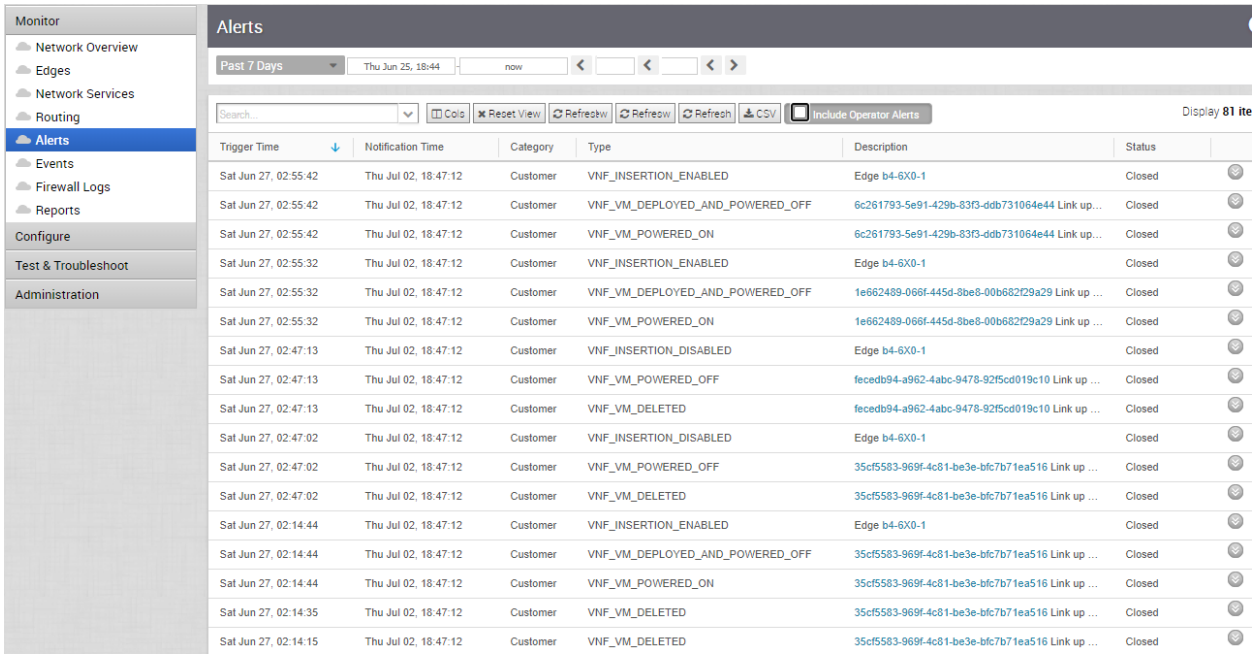
- **Edge-VNF-VM-Bereitstellung (Edge VNF Virtual Machine Deployment)** – Sie erhalten eine Warnung, wenn sich der Status der Edge-VNF-VM-Bereitstellung ändert.

- **Edge-VNF-Einfügung (Edge VNF Insertion)** – Sie erhalten eine Warnung, wenn sich der Status der Edge-VNF-Bereitstellung ändert.
- **Edge-VNF-Image-Downloadereignis (Edge VNF Image Download Event)** – Sie erhalten eine Warnung, wenn sich der Status des Edge-VNF-Image-Downloads ändert.

Sie können die Warnbenachrichtigungen auf der Seite **Überwachen (Monitor) > Warnungen (Alerts)** anzeigen.

Um die Warnungen im Zusammenhang mit VNF anzuzeigen, können Sie die Filteroption verwenden. Klicken Sie auf den Dropdown-Pfeil neben der Option **Suchen (Search)** und wählen Sie aus, dass nach Typ gefiltert werden soll.

In der folgenden Abbildung sind einige der VNF-Warnungen dargestellt.



Sie können die Warnungen auch auf der neuen Benutzeroberfläche von Orchestrator anzeigen.

Klicken Sie im Popup-Fenster auf **Neue Orchestrator-Benutzeroberfläche starten (Launch New Orchestrator UI)**. Die Benutzeroberfläche wird auf einer neuen Registerkarte geöffnet, auf der die Überwachungsoptionen angezeigt werden. Klicken Sie auf **Warnungen (Alerts)**. Klicken Sie in der Option **Suchen (Search)** auf das Filtersymbol, um die VNF-Warnungen zu filtern.

Konfigurieren der Edge-Unternehmensrichtlinie

In diesem Abschnitt wird beschrieben, wie Sie die Edge-Unternehmensrichtlinie konfigurieren.

Konfigurieren der Edge-Unternehmensrichtlinie

Die Edge-Firewall verwendet in erster Linie Regeln aus dem zugewiesenen Profil. Das Außerkraftsetzen der Regeln für die Profil-Unternehmensrichtlinie auf dem Edge ist ein optionaler Schritt.

Außerkraftsetzen der Regeln für die Unternehmensrichtlinie

Auf dem Edge können die Regeln für die Unternehmensrichtlinie aus dem zugewiesenen Profil mit Hilfe des unten gezeigten Dialogfelds „Edge-Unternehmensrichtlinie (Edge Business Policy)“ außer Kraft gesetzt werden. Jeder Übereinstimmungswert für die Außerkraftsetzung der Unternehmensrichtlinie, der mit einer Regel für die Profil-Unternehmensrichtlinie übereinstimmt, setzt diese Profilregel außer Kraft. Sie können Außerkraftsetzungsregeln auf dieselbe Weise erstellen, wie Sie Profilregeln erstellen (siehe Kapitel 11 Konfigurieren der Unternehmensrichtlinie für ein Profil).

Wie in der Abbildung unten gezeigt, ist die Unternehmensrichtlinie segmentierfähig. Alle für die Konfiguration verfügbaren Segmente werden im Dropdown-Menü **Segment konfigurieren (Configure Segment)** aufgelistet.

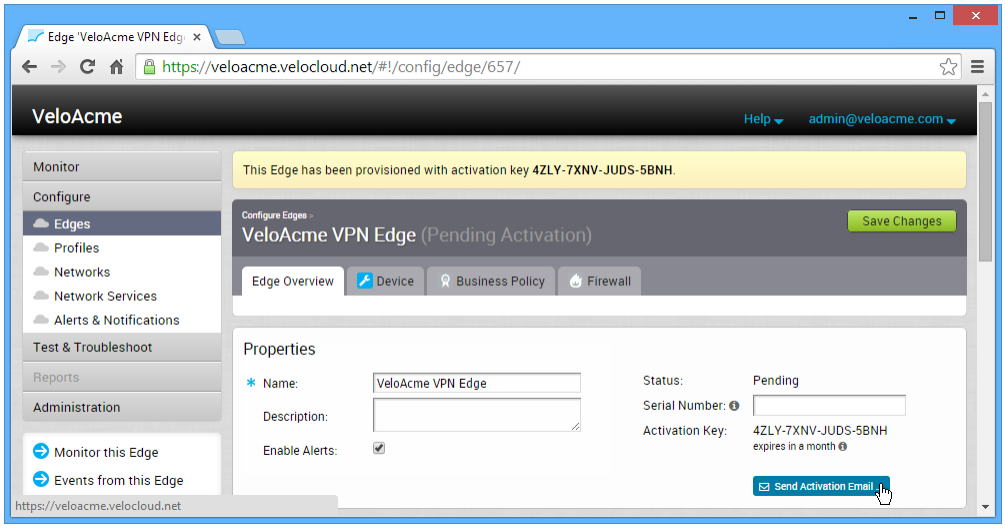
Wenn Sie ein zu konfigurierendes Segment aus der Dropdown-Liste **Segment konfigurieren (Configure Segment)** auswählen, werden die mit diesem Segment verbundenen Einstellungen und Optionen im Bereich **Segmente konfigurieren (Configure Segments)** angezeigt. **Globales Segment [Normal] (Global Segment [Regular])** ist das Standardsegment.

Weitere Informationen zur Segmentierung finden Sie unter Kapitel 7 Konfigurieren von Segmenten und *Konfigurieren des Edge-Geräts*.

Konfigurieren der Edge-Aktivierung

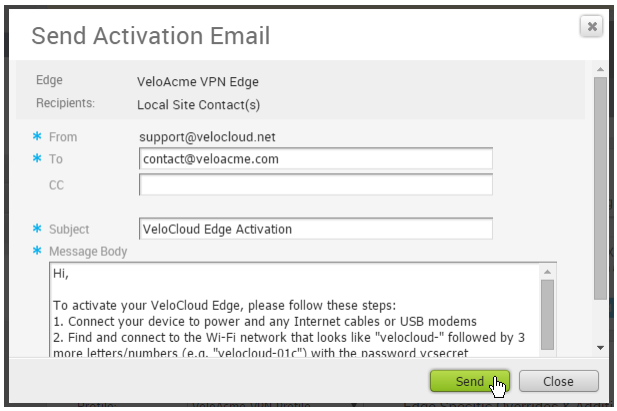
In diesem Abschnitt wird die Initiierung der Edge-Aktivierung beschrieben.

Nach dem Speichern einer Edge-Konfiguration wird dieser ein Aktivierungsschlüssel zugewiesen. Sie starten die Edge-Aktivierung, indem Sie auf den Link **Aktivierungs-E-Mail senden (Send Activation Email)** auf der Registerkarte **Edge-Übersicht (Edge Overview)** klicken.



Das Dialogfeld **Aktivierungs-E-Mail senden (Send Activation Email)** wird mit einem E-Mail-Vorschlag zum Senden an einen Site-Kontakt geöffnet. Dem Site-Kontakt werden einfache Anweisungen zum Herstellen einer Verbindung mit und Aktivieren der Edge-Hardware bereitgestellt. Geben Sie in der E-Mail zusätzliche Anweisungen zum Verbinden von WAN- und LAN-Netzwerken einer speziellen Site mit der Edge an.

Hinweis Wenn in Version 3.4 ein Edge 510 LTE-Gerät konfiguriert wurde, enthält die Aktivierungs-E-Mail Mobilfunkeinstellungen (z. B. SIM-PIN, Netzwerk, APN, Benutzername).



Hinweis Wenn Sie das Edge 510 LTE-Gerät konfigurieren, können Sie zu Fehlerbehebungszwecken den Diagnosetest „LTE-Modeminformationen (LTE Modem Information)“ ausführen. Während des Diagnosetests **LTE-Modeminformationen (LTE Modem Information)** werden Diagnoseinformationen abgerufen, wie z. B. Signalstärke, Verbindungsinformationen usw. Informationen zum Ausführen eines Diagnosetests finden Sie im Abschnitt Remote-Diagnose.

LAN-seitige NAT-Regeln auf Edge-Ebene

Mithilfe LAN-seitiger NAT-Regeln können Sie IP-Adressen in einem nicht angekündigten Netzwerk in IP-Adressen in einem angekündigten Netzwerk übersetzen. Für die Profil- und Edge-Ebene wurden innerhalb der Konfiguration der Geräteeinstellungen LAN-seitige NAT-Regeln in Version 3.3.2 eingeführt. Als Erweiterung wurde in Version 3.4 LAN-seitige NAT basierend auf Quelle und Ziel sowie Unterstützung für Quell- und Ziel-NAT desselben Pakets eingeführt.

Ab Version 3.3.2 wurde in VMware SD-WAN ein neues LAN-seitiges NAT-Modul für NAT-VPN-Routen auf dem Edge eingeführt. Die Hauptanwendungsfälle lauten wie folgt:

- Branch-überlappende IP aufgrund von M&A
- Ausblenden der privaten IP eines Branch oder Datencenters aus Sicherheitsgründen

In Version 3.4 werden zusätzliche Konfigurationsfelder für weitere Anwendungsfälle eingeführt. Im Folgenden finden Sie eine allgemeine Übersicht hinsichtlich der Unterstützung LAN-seitiger NAT in verschiedenen Versionen:

- Quell- oder Ziel-NAT für alle übereinstimmenden Subnetze, sowohl 1:1 als auch Viele:1 werden unterstützt (Version 3.3.2)
- Quell-NAT basierend auf Zielsubnetz oder Ziel-NAT basierend auf Quellsubnetz, sowohl 1:1 als auch Viele:1 werden unterstützt (Version 3.4)
- Quell-NAT und 1:1-Ziel-NAT im selben Paket (Version 3.4)

Hinweis

- Unterstützung für Quell- und Ziel-NAT vom Typ „Viele:1“ und „1:1“ (z. B. /24 zu /24).
- Wenn mehrere Regeln konfiguriert sind, wird nur die erste übereinstimmende Regel ausgeführt.
- LAN-seitige NAT wird vor der Routen- oder Flow-Suche durchgeführt. Um Datenverkehr im Unternehmensprofil abzugleichen, müssen Benutzer die per NAT umgesetzte IP verwenden.
- Standardmäßig werden per NAT umgesetzte IPs nicht über den Edge angekündigt. Stellen Sie deshalb sicher, dass Sie die statische Route für die per NAT umgesetzte IP hinzufügen und beim Overlay ankündigen.
- Konfigurationen in Version 3.3.2 werden übernommen. Beim Upgrade auf Version 3.4 muss keine Neukonfiguration durchgeführt werden.

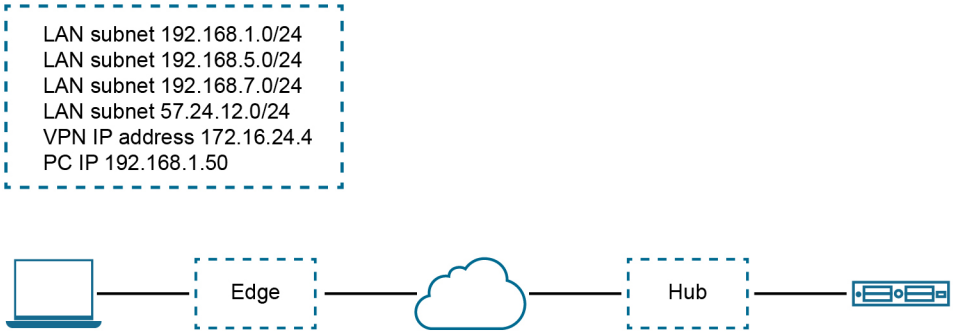
LAN-seitige NAT (Version 3.3.2)

Anwendungsfall Nr. 1: Quell-NAT vom Typ „Viele:1“

In diesem Szenario hat ein Drittanbieter der Site eines Kunden mehrere nicht überlappende Subnetze zugewiesen. Der Server im Datencenter des Kunden erkennt den Datenverkehr dieses Drittanbieters anhand einer einzelnen IP-Adresse an einer bestimmten Site.

Die für Anwendungsfall Nr. 1 für Version 3.3.2 benötigte Konfiguration: Neue Regel: LAN-seitige NAT 192.168.1.0/24 -> 172.16.24.4/32

Wie in folgender Abbildung angezeigt, wird der TCP- und UDP-Datenverkehr per PAT umgesetzt, da es sich bei der NAT-Regel um eine einzelne IP handelt. Aus diesem Grund wird in diesem Beispiel 192.168.1.50 zu 172.16.24.4 mit einem flüchtigen Quellport für TCP-/UDP-Datenverkehr, ICMP-Datenverkehr wird zu 172.16.24.4 mit einer benutzerdefinierten ICMP-ID für Reverse-Lookup, und der gesamte andere Datenverkehr wird gelöscht.

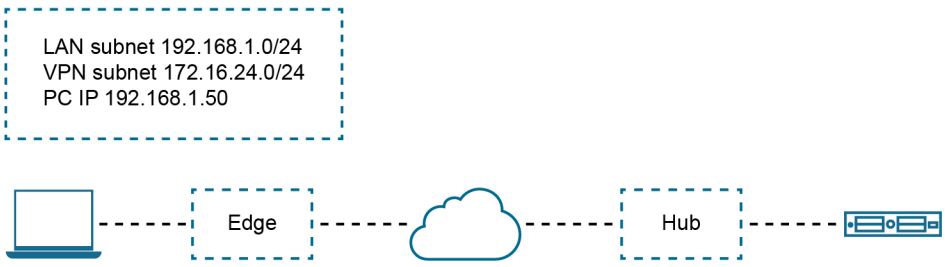


Anwendungsfall Nr. 2: Quell-NAT vom Typ „1:1“

In diesem Szenario fungiert 192.168.1.0/24 als LAN-Subnetz. Hierbei handelt es sich jedoch um ein Subnetz, das mit anderen Sites überlappt. Ein eindeutiges Subnetz gleicher Größe, 172.16.24.0/24, wurde zur Verwendung für VPN-Kommunikation an dieser Site zugewiesen. Der Datenverkehr des PC muss vor der Routensuche per NAT auf dem Edge umgesetzt werden. Andernfalls stimmt die Quellroute mit 192.168.1.0/24 überein und wird nicht von diesem Edge angekündigt. Folglich wird der Datenverkehr gelöscht.

Die für Anwendungsfall Nr. 2 benötigte Konfiguration: Neue Regel: LAN-seitige NAT 192.168.1.0/24 -> 172.16.24.0/24

Da die Größe der Subnetze übereinstimmt, werden alle der Subnetzmaske entsprechenden Bits per NAT umgesetzt. Deshalb wird in der folgenden Abbildung 192.168.1.50 zu 172.16.24.50.

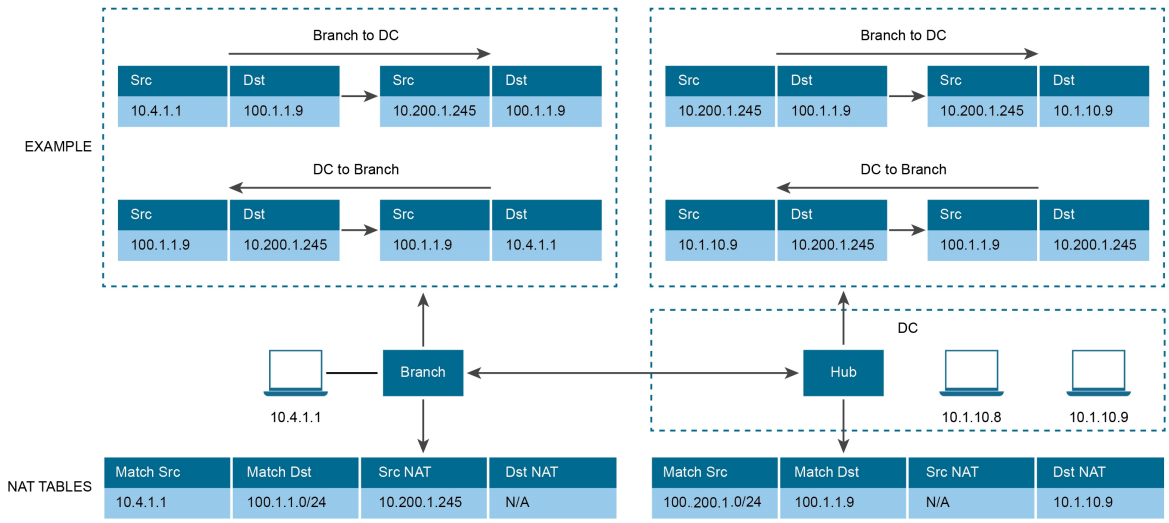


LAN-seitige NAT basierend auf Quelle oder Ziel (Version 3.4)

In Version 3.4 wird LAN-seitige NAT auf der Basis von Quell-/Zielunterstützung als Teil einer einzelnen Regel eingeführt, in der NAT nur für eine Teilmenge des Datenverkehrs auf der Grundlage von Quell- oder Zielsubnetzen aktiviert werden kann. Weitere Informationen zu dieser Verbesserung finden Sie in den folgenden Anwendungsfällen.

Anwendungsfall Nr. 1: „Durchführen von SNAT oder DNAT mit Quelle und Ziel als Übereinstimmungskriterien“

In folgendem Beispiel sollte der Branch die Quell-IP 10.4.1.1 nur für den Datenverkehr per NAT in 10.200.1.245 umsetzen, der für 100.1.1.0/24 bestimmt ist.Ebenso sollte im DC die Ziel-IP 100.1.1.9 nur dann per NAT in 10.1.10.9 umgesetzt werden, wenn der Datenverkehr aus der Quelle 10.200.1.0/24 empfangen wird.



Weitere Informationen finden Sie in der folgenden Abbildung (LAN-seitige NAT-Regeln für den Branch).

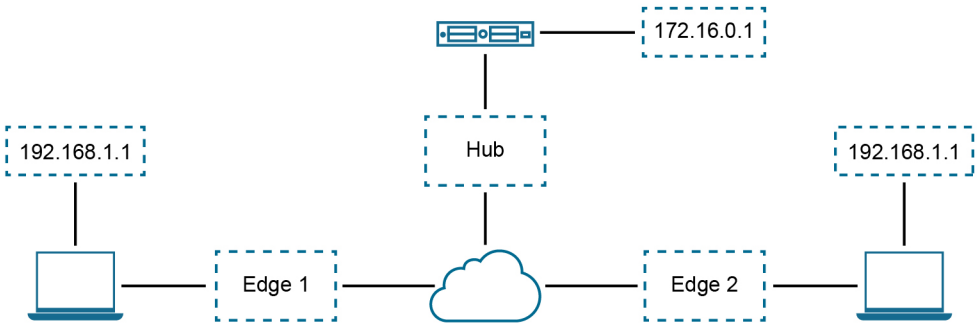
Weitere Informationen finden Sie in der folgenden Abbildung (LAN-seitige NAT-Regeln für den Hub).

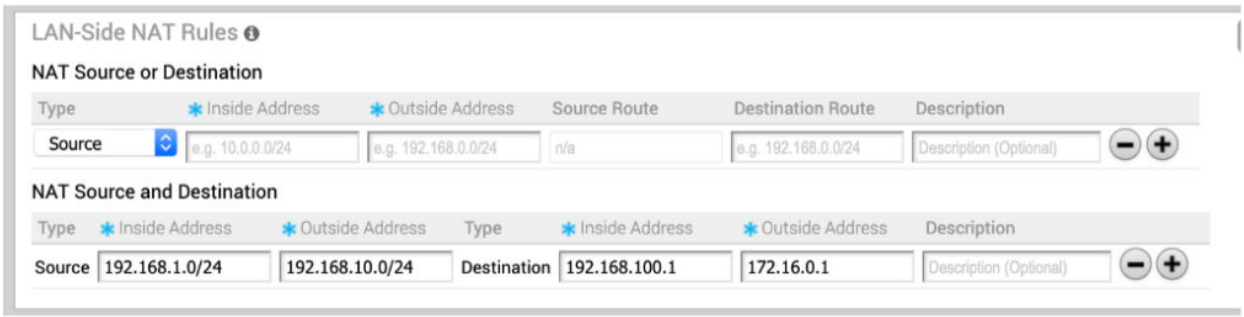
Hub:

Anwendungsfall Nr. 2: Sowohl Quell- als auch Ziel-IP per NAT im Paket umsetzen

Betrachten Sie folgendes Szenario. In diesem Beispiel wird jeder Site im Netzwerk dasselbe Subnetz zugewiesen, sodass das Branch-LAN auf jeder Site identisch ist. „PC1“ und „PC2“ verfügen über dieselbe IP-Adresse und müssen beide mit einem Server hinter dem Hub kommunizieren. Der Datenverkehr muss per Quell-NAT umgesetzt werden, damit überlappende IP-Adressen verwendet werden können, wie z. B. in Edge 1 sollten PCs (192.168.1.0/24) per NAT in 192.168.10.0/24 umgesetzt werden, in Edge2 sollten PCs (192.168.1.0/24) per NAT in 192.168.20.0/24 umgesetzt werden.

Ebenso sollte aus Sicherheitsgründen der Server hinter dem Hub mit der realen IP „172.16.0.1“ den PCs als „192.168.100.1“ präsentiert werden. Des Weiteren sollte diese IP nicht zwischen dem Hub und Edge an SD-WAN verteilt werden, Regeln mit einer Kombination aus Quelle und Ziel sind auf demselben Edge erforderlich.





Hinweis LAN-seitige NAT-Regeln können auf Profil- oder Edge-Ebene konfiguriert werden. Für eine Konfiguration auf Edge-Ebene stellen Sie sicher, dass das Kontrollkästchen **Edge-Außerkraftsetzung aktivieren (Enable Edge Override)** markiert ist.

Verfahren konfigurieren

Hinweis: Wenn der Benutzer die Standardregel „Alle“ definieren möchte, müssen die IP-Adresse und das Präfix aus Nullen bestehen: 0.0.0.0/0.

So wenden Sie LAN-seitige NAT-Regeln an:

1 Wechseln Sie im Navigationsbereich zu **Konfigurieren (Configure) > Edges**.

2 Führen Sie auf der Registerkarte **Geräteeinstellungen (Device Settings)** einen Bildlauf zum Bereich **LAN-seitige NAT-Regeln (LAN-Side NAT Rules)** durch.

3 Geben Sie im Bereich **LAN-seitige NAT-Regeln (LAN-Side NAT Rules)** im Abschnitt „NAT-Quelle oder -Ziel (NAT Source or Destination)“ Folgendes ein: (Eine Beschreibung der Felder in den folgenden Schritten finden Sie in nachstehender Tabelle.)

   a Geben Sie eine Adresse im Textfeld **Innere Adresse (Inside Address)** ein.

   b Geben Sie eine Adresse im Textfeld **Äußere Adresse (Outside Address)** ein.

   c Geben Sie die Quellroute im entsprechenden Textfeld ein.

   d Geben Sie die Zielroute im entsprechenden Textfeld ein.

   e Geben Sie eine Beschreibung für die Regel im Textfeld **Beschreibung (Description)** ein (optional).

4 Geben Sie im Bereich **LAN-seitige NAT-Regeln (LAN-Side NAT Rules)** Folgendes für die NAT-Quelle und das NAT-Ziel ein: (Eine Beschreibung der Felder in den folgenden Schritten finden Sie in nachstehender Tabelle.)

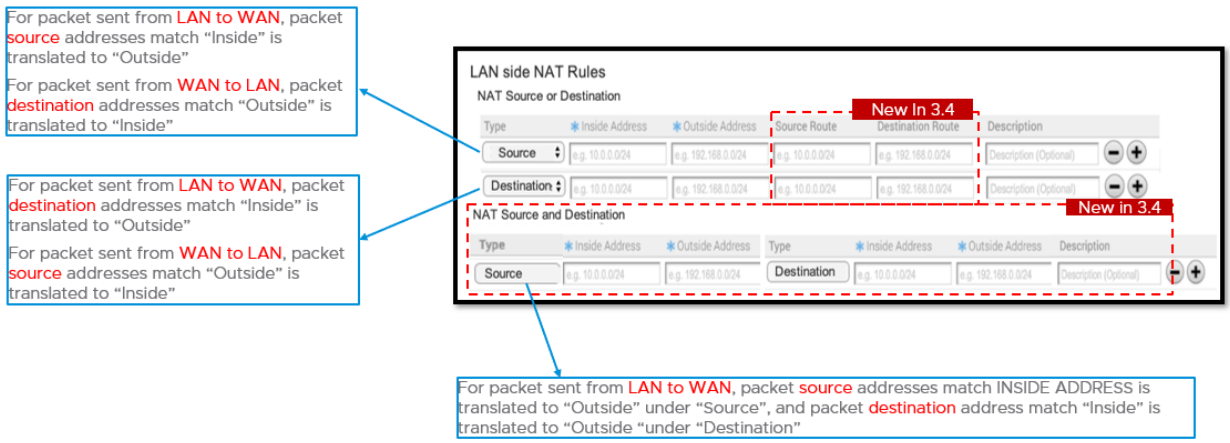
   a Geben Sie für den Typ **Quelle (Source)** die **Innere Adresse (Inside Address)** und die **Äußere Adresse (Outside Address)** in den entsprechenden Textfeldern ein.

   b Geben Sie für den Typ **Ziel (Destination)** die **Innere Adresse (Inside Address)** und die **Äußere Adresse (Outside Address)** in den entsprechenden Textfeldern ein.

   c Geben Sie eine Beschreibung für die Regel im Textfeld **Beschreibung (Description)** ein (optional).

LAN-seitige NAT-Regel	Typ	Beschreibung
Dropdown-Menü „Typ (Type)“	Entweder „Quelle (Source)“ oder „Ziel (Destination)“ auswählen	Geben Sie an, ob diese NAT-Regel auf die Quell- oder Ziel-IP-Adresse des Benutzerdatenverkehrs angewendet werden soll.
Textfeld „Innere Adresse (Inside Address)“	IPv4-Adresse/Präfix, Präfix muss zwischen 1 und 32 liegen.	Die „innere“ oder „Vor NAT“-IP-Adresse (bei einem Präfix von 32) oder das Subnetz (bei einem Präfix kleiner als 32).
Textfeld „Äußere Adresse (Outside Address)“	IPv4-Adresse/Präfix, Präfix muss zwischen 1 und 32 liegen.	Die „äußere“ oder „Nach NAT“-IP-Adresse (bei einem Präfix von 32) oder das Subnetz (bei einem Präfix kleiner als 32).

LAN-seitige NAT-Regel	Typ	Beschreibung
Textfeld „Quellroute (Source Route)“	- Optional - IPv4-Adresse/Präfix - Präfix muss zwischen 1 und 32 liegen - Standard: beliebig	Geben Sie Quell-IP/Subnetz als Übereinstimmungskriterien für die Ziel-NAT an. Nur gültig, wenn der Typ „Ziel (Destination)“ lautet.
Textfeld „Zielroute (Destination Route)“	- Optional - IPv4-Adresse/Präfix - Präfix muss zwischen 1 und 32 liegen - Standard: beliebig	Geben Sie Ziel-IP/Subnetz als Übereinstimmungskriterien für die Quell-NAT an.Nur gültig, wenn der Typ „Quelle (Source)“ lautet.
Textfeld „Beschreibung (Description)“	Text	Benutzerdefiniertes Textfeld zur Beschreibung der NAT-Regel.



Hinweis **Wichtig:** Wenn das innere Präfix kleiner ist als das äußere Präfix, unterstützen Sie Viele:1-NAT in der LAN-zu-WAN-Richtung und 1:1-NAT in der WAN-zu-LAN-Richtung. Beispiel: Wenn 10.0.5.0/24 der inneren Adresse und 192.168.1.25/32 der äußeren Adresse entspricht und „Quelle “ als Typ fungiert, wird für Sitzungen von LAN zu WAN mit der Quell-IP, die der inneren Adresse entspricht, 10.0.5.1 in 192.168.1.25 übersetzt. Für Sitzungen von WAN zu LAN mit der Ziel-IP, die der äußeren Adresse entspricht, wird 192.168.1.25 in 10.0.5.25 übersetzt. Wenn das innere Präfix größer ist als das äußere Präfix, unterstützen Sie gleichfalls Viele:1-NAT in der WAN-zu-LAN-Richtung und 1:1-NAT in der LAN-zu-WAN-Richtung. Die über NAT umgesetzte IP wird nicht automatisch angekündigt. Stellen Sie sicher, dass eine statische Route für die über NAT umgesetzte IP konfiguriert wird und der nächste Hop als LAN-IP des Quellsubnetzes fungiert.

Merkblatt für LAN-seitige NAT

Anwendungsbeispiel 1:

- **Richtung des Datenverkehrs:** LAN->WAN
- **Zu übersetzendes Element:** Quelladresse des Pakets

- **Konfigurationszuordnung:**
  - NAT-Typ = „Quelle“
  - Ursprüngliche IP = „Innere Adresse“
  - NAT-IP = „Äußere Adresse“

NAT-Typ	Innen	Außerhalb	Typ	LAN->WAN
Quelle (Source)	A.0/24	B.0/24	1:1	A.1 wird in B.1 übersetzt, A.2 in B.2 usw.
Quelle (Source)	A.0/24	B.1/32	Viele:1	A.1 und A.2 werden in B.1 übersetzt
Quelle (Source)	A.1/32	B.0/24	1:1	A.1 wird in B.1 übersetzt, weitere B.X werden nicht verwendet

Anwendungsbeispiel 2:

- **Richtung des Datenverkehrs:** WAN -> LAN
- **Zu übersetzendes Element:** Zieladresse des Pakets
- **Konfigurationszuordnung:**
  - NAT-Typ = „Quelle“
  - Ursprüngliche IP = „Äußere Adresse“
  - NAT-IP = „Innere Adresse“

NAT-Typ	Innen	Außerhalb	Typ	WAN->LAN
Quelle	A.0/24	B.0/24	1:1	B.1 wird in A.1 übersetzt, B.2 in A.2 usw.
Quelle	A.0/24	B.1/32	Viele:1	B.1 wird in A.1 übersetzt
Quelle	A.1/32	B.0/24	1:Viele	B.1 und B.2 werden in A.1 übersetzt

Anwendungsbeispiel 3:

- **Richtung des Datenverkehrs:** LAN->WAN
- **Zu übersetzendes Element:** Zieladresse des Pakets
- **Konfigurationszuordnung:**
  - NAT-Typ = „Ziel“
  - Ursprüngliche IP = „Innere Adresse“

- NAT-IP = „Äußere Adresse“

NAT-Typ	Innerhalb	Außerhalb	Typ	LAN->WAN
Ziel (Destination)	A.0/24	B.0/24	1:1	A.1 wird in B.1 übersetzt, A.1 in B.2 usw.
Ziel (Destination)	A.0/24	B.1/32	Viele:1	A.1 und A.2 werden in B.1 übersetzt
Ziel (Destination)	A.1/32	B.0/24	1:Viele	A.1 wird in B.1 übersetzt

Anwendungsbeispiel 4:

- **Richtung des Datenverkehrs:** WAN->LAN
- **Zu übersetzendes Element:** Quelladresse des Pakets
- **Konfigurationszuordnung:**
  - NAT-Typ = „Ziel“
  - Ursprüngliche IP = „Äußere Adresse“
  - NAT-IP = „Innere Adresse“

NAT-Typ	Innen	Außerhalb	Typ	WAN->LAN
Ziel	A.0/24	B.0/24	1:1	B.1 wird in A.1 übersetzt, B.2 in A.2 usw.
Ziel (Destination)	A.0/24	B.1/32	Viele:1	B.1 wird in A.1 übersetzt
Ziel	A.1/32	B.0/24	1:Viele	B.1 und B.2 werden in A.1 übersetzt

Objektgruppen

17

Eine Objektgruppe besteht aus einem Bereich von IP-Adressen oder Portnummern. Wenn Sie Unternehmensrichtlinien und Firewallregeln erstellen, können Sie die Regeln für einen Bereich von IP-Adressen oder einen Bereich von TCP/UDP-Ports definieren, indem Sie die Objektgruppen in die Regeldefinitionen einschließen.

Sie können Adressgruppen erstellen, um den Bereich der gültigen IP-Adressen und Portgruppen für den Bereich der Portnummern einzusparen. Sie können die Richtlinienverwaltung vereinfachen, indem Sie Objektgruppen bestimmter Typen erstellen und diese in Richtlinien und Regeln erneut verwenden.

Mithilfe von Objektgruppen können Sie:

- Richtlinien problemlos verwalten
- Die Richtlinienkomponenten modularisieren und wiederverwenden
- Alle referenzierten Geschäfts- und Firewallrichtlinien problemlos aktualisieren
- Die Anzahl der Richtlinien reduzieren
- Die Fehlerbehebung und die Lesbarkeit der Richtlinie verbessern

Hinweis Sie können Objektgruppen erstellen, aktualisieren oder löschen, wenn Sie über Berechtigungen zum Erstellen, Aktualisieren oder Löschen für das Objekt NETWORK_SERVICE verfügen. Sie können die Objektgruppen nur anzeigen, wenn Sie über Leseberechtigungen für die Objekte NETWORK_SERVICE und ENTERPRISE_PROFILE verfügen.

Dieses Kapitel enthält die folgenden Themen:

Konfigurieren von Adressgruppen

Adressgruppen können einen Bereich von IP-Adressen mit unterschiedlichen Optionen speichern.

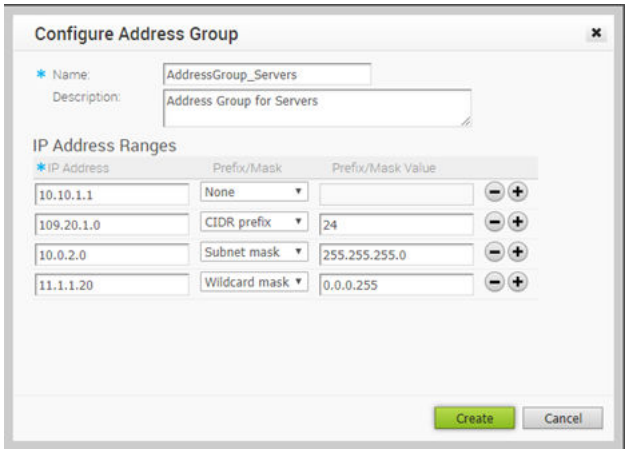
Verfahren

1 Klicken Sie im Unternehmensportal auf **Konfigurieren (Configure) > Objektgruppen (Object Groups)**.

2 Klicken Sie auf der Registerkarte **Adressgruppen (Address Groups)** auf **Aktionen (Actions) > Neu (New)**.

3 Geben Sie im Fenster **Adressgruppe konfigurieren (Configure Address Group)** einen Namen und eine Beschreibung für die Adressgruppe ein.

4 Geben Sie den Bereich der IP-Adressen nach Bedarf ein.



5 Klicken Sie auf **Erstellen (Create)**.

Nächste Schritte

Sie können eine Unternehmensrichtlinie oder eine Firewallregel mit der Adressgruppe definieren, um den Bereich der IP-Adressen in die Adressgruppe aufzunehmen.

Sie können die IP-Adressen in einer Adressgruppe hinzufügen oder ändern, indem Sie auf der Registerkarte „Adressgruppen (Address Groups)“ auf **Aktionen (Actions) > Aktualisieren (Update)** klicken.

Wenn Sie eine Adressgruppe löschen möchten, müssen Sie sicherstellen, dass die Adressgruppe von den Unternehmensrichtlinien oder Firewallregeln ausgeschlossen wird.

Konfigurieren von Portgruppen

Portgruppen können einen Bereich von TCP- und UDP-Portnummern speichern.

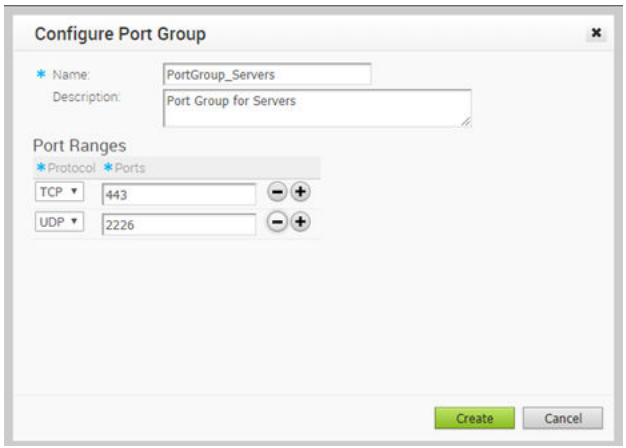
Verfahren

1 Klicken Sie im Unternehmensportal auf **Konfigurieren (Configure) > Objektgruppen (Object Groups)**.

2 Klicken Sie auf der Registerkarte **Portgruppen (Port Groups)** auf **Aktionen (Actions) > Neu (New)**.

3 Geben Sie im Fenster **Portgruppe konfigurieren (Configure Port Group)** einen Namen und eine Beschreibung für die Portgruppe ein.

4 Wählen Sie das Protokoll als TCP oder UDP aus und geben Sie die entsprechenden Portnummern nach Bedarf ein.



5 Klicken Sie auf **Erstellen (Create)**.

Nächste Schritte

Sie können mit der Port-Gruppe eine Unternehmensrichtlinie oder eine Firewall-Regel definieren, um den Bereich der Portnummern einzubeziehen.

Sie können die Portnummern in einer Portgruppe hinzufügen oder ändern, indem Sie auf der Registerkarte „Portgruppen (Port Groups)“ auf **Aktionen (Actions) > Aktualisieren (Update)** klicken.

Wenn Sie eine Port-Gruppe löschen möchten, stellen Sie sicher, dass die Portgruppe aus den Unternehmensrichtlinien oder Firewallregeln ausgeschlossen wird.

Konfigurieren von Unternehmensrichtlinien mit Objektgruppen

Beim Konfigurieren von Unternehmensrichtlinien können Sie die vorhandenen Objektgruppen auswählen, die der Quelle oder dem Ziel entsprechen. Dazu gehört der Bereich von IP-Adressen oder Portnummern, der in den Objektgruppen der Definition der Unternehmensrichtlinie zur Verfügung steht.

Weitere Informationen zu Unternehmensrichtlinien finden Sie unter *Konfigurieren der Profil-Unternehmensrichtlinie*.

Verfahren

1 Klicken Sie im Unternehmensportal auf **Konfigurieren (Configure) > Profile (Profiles)**.

2 Wählen Sie ein Profil aus der Liste aus und klicken Sie auf die Registerkarte **Unternehmensrichtlinie (Business Policy)**.

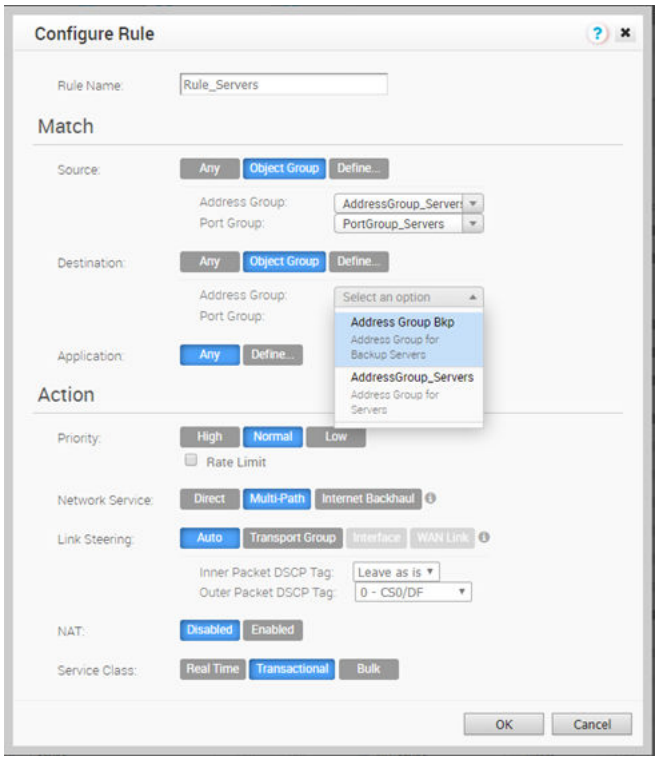
3 Klicken Sie auf **Neue Regel (New Rule)** oder **Aktionen (Actions) > Neue Regel (New Rule)**.

4 Geben Sie einen Namen für die Unternehmensrichtlinie ein.

5 Klicken Sie im Bereich **Übereinstimmung (Match)** auf **Objektgruppe (Object Group)** für die Quelle.

6 Wählen Sie in der Dropdown-Liste die relevante Adressgruppe und Portgruppe aus.

7 Falls erforderlich, können Sie auch die Adresse und die Portgruppen für das Ziel auswählen.



8 Wählen Sie die erforderlichen weiteren Aktionen aus und klicken Sie auf **OK**.

Ergebnisse

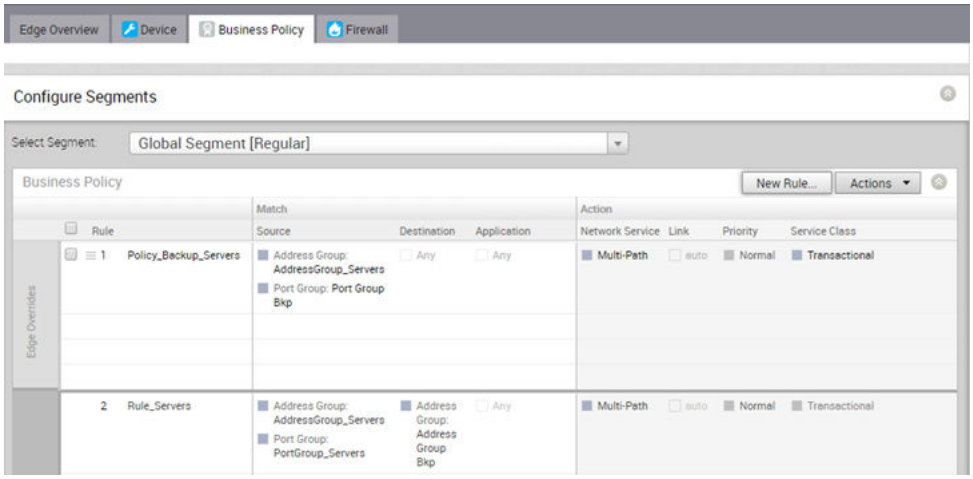
Die Unternehmensrichtlinien, die Sie für ein Profil erstellen, werden automatisch auf alle dem Profil zugeordneten Edges angewendet. Falls erforderlich, können Sie zusätzliche Unternehmensrichtlinien speziell für die Edges erstellen.

1 Navigieren Sie zu **Konfigurieren (Configure) > Edges**, wählen Sie einen Edge aus und klicken Sie auf die Registerkarte **Unternehmensrichtlinie (Business Policy)**.

2 Klicken Sie auf **Neue Regel (New Rule)** oder **Aktionen (Actions) > Neue Regel (New Rule)**.

3 Definieren Sie die Regel mit relevanten Objektgruppen und anderen Aktionen.

Auf der Registerkarte „Unternehmensrichtlinie (Business Policy)“ des Edge werden die Richtlinien aus dem zugehörigen Profil zusammen mit den für den Edge spezifischen Richtlinien angezeigt.



Hinweis Standardmäßig werden die Unternehmensrichtlinien dem globalen Segment zugewiesen. Falls erforderlich, können Sie ein Segment aus der Dropdown-Liste **Segment auswählen (Select Segment)** wählen und Unternehmensrichtlinien speziell für das ausgewählte Segment erstellen.

Nächste Schritte

Sie können die Objektgruppen mit zusätzlichen IP-Adressen und Portnummern ändern. Die Änderungen werden automatisch in die Unternehmensrichtlinien aufgenommen, die die Objektgruppen verwenden.

Konfigurieren von Firewallregeln mit Objektgruppen

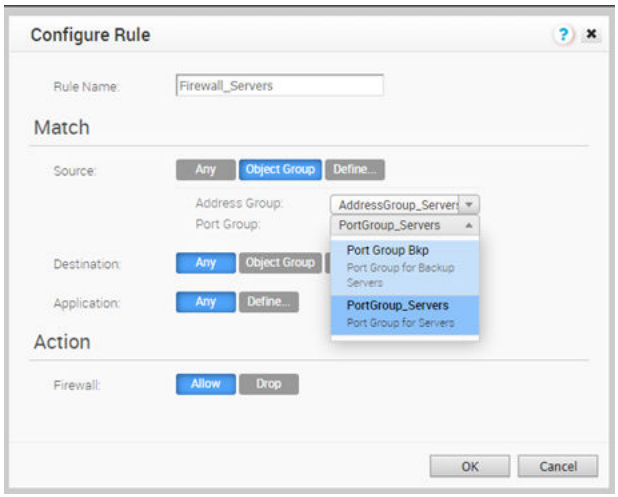
Beim Konfigurieren von Firewallregeln können Sie die vorhandenen Objektgruppen auswählen, die der Quelle oder dem Ziel entsprechen. Dies umfasst den Bereich der IP-Adressen oder Portnummern, die in den Objektgruppen in den Regeln verfügbar sind.

Weitere Informationen zu Firewallregeln finden Sie unter *Konfigurieren von Firewallregeln*.

Verfahren

1. Klicken Sie im Unternehmensportal auf **Konfigurieren (Configure) > Profile (Profiles)**.
2. Wählen Sie ein Profil aus der Liste aus und klicken Sie auf die Registerkarte **Firewall**.
3. Klicken Sie auf **Neue Regel (New Rule)** oder **Aktionen (Actions) > Neue Regel (New Rule)**.
4. Geben Sie einen Dateinamen für die Firewallregel ein.
5. Klicken Sie im Bereich **Übereinstimmung (Match)** auf **Objektgruppe (Object Group)** für die Quelle.
6. Wählen Sie in der Dropdown-Liste die relevante Adressgruppe und Portgruppe aus.

7 Falls erforderlich, können Sie auch die Adresse und die Portgruppen für das Ziel auswählen.



8 Wählen Sie die erforderliche Maßnahme aus und klicken Sie auf **OK**.

Ergebnisse

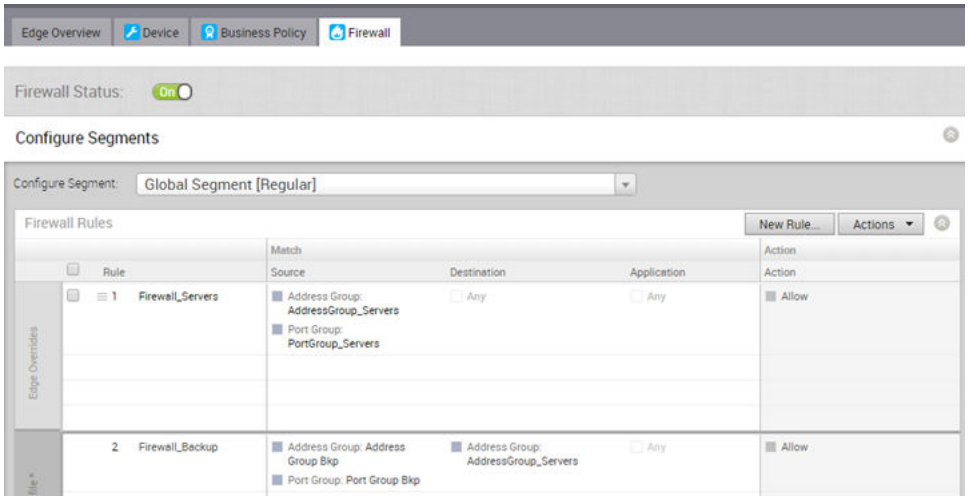
Die Firewallregeln, die Sie für ein Profil erstellen, werden automatisch auf alle Edges angewendet, die mit dem Profil verknüpft sind. Bei Bedarf können Sie zusätzliche Edge-spezifische Regeln erstellen.

1 Navigieren Sie zu **Konfigurieren (Configure) > Edges**, wählen Sie einen Edge aus und klicken Sie auf die Registerkarte **Firewall**.

2 Klicken Sie auf **Neue Regel (New Rule)** oder **Aktionen (Actions) > Neue Regel (New Rule)**.

3 Definieren Sie die Regel mit relevanten Objektgruppen und anderen Aktionen.

Auf der Registerkarte „Firewall“ des Edge werden die Firewallregeln aus dem zugehörigen Profil zusammen mit den Edge-spezifischen Regeln angezeigt.



Hinweis Standardmäßig werden die Firewallregeln dem globalen Segment zugewiesen. Falls erforderlich, können Sie ein Segment aus der Dropdown-Liste **Segment auswählen (Select Segment)** auswählen und Firewallregeln erstellen, die spezifisch für das ausgewählte Segment sind.

Nächste Schritte

Sie können die Objektgruppen mit zusätzlichen IP-Adressen und Portnummern ändern. Die Änderungen werden automatisch in die Firewallregeln aufgenommen, die die Objektgruppen verwenden.

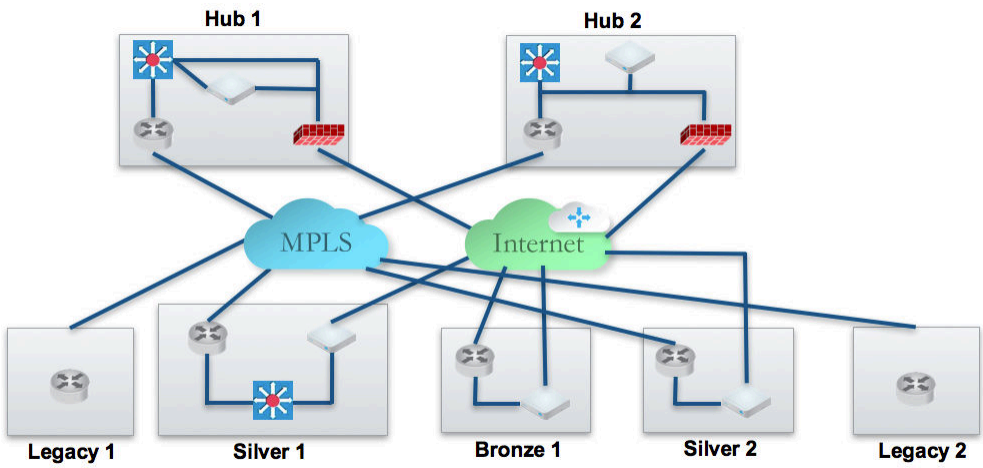
Site-Konfigurationen

18

Topologien für Datencenter, die einen SD-WAN Hub und VMware SD-WAN-Branch-Konfigurationen (Branches Gold, Silver und Bronze) beinhalten, werden unter Verwendung von MPLS- und Internetverbindungen konfiguriert. Legacy-Branch-Konfigurationen (diejenigen ohne SD-WAN Edge) sind enthalten, und die Hub- und Branch-Konfiguration werden bei Vorhandensein der Legacy-Branches geändert.

Das folgende Diagramm zeigt eine Beispieltopologie, die zwei Datencenter-Hubs und die Gold-, Silver- und Bronze-Varianten der Branch-Topologien umfassen, die über MPLS und das Internet miteinander verbunden sind. In diesem Beispiel werden die einzelnen Aufgaben beschrieben, die für Datencenter- und Branch-Konfigurationen erforderlich sind. Es wird vorausgesetzt, dass Sie mit Konzepten und Konfigurationsdetails in früheren Abschnitten dieser Dokumentation vertraut sind. Dieser Abschnitt konzentriert sich in erster Linie auf die Konfiguration von Netzwerken, Profilgeräteeinstellungen und die für jede Topologie erforderliche Edge-Konfiguration.

Zusätzliche Konfigurationsschritte für die Umleitung des Datenverkehrs, das Steuerungs-Routing (z. B. für Backhaul-Datenverkehr und VPNs) und für das Edge-Failover werden ebenfalls behandelt.



Dieser Abschnitt konzentriert sich in erster Linie auf die Konfiguration, die für eine Topologie erforderlich ist, die verschiedene Arten von Datencenter- und Branch-Standorten umfasst. Erläutert werden die Netzwerk-, Profil/Edge-Geräteeinstellungen und Profil/Edge-Business-Richtlinien, die zur Durchführung der Konfigurationen erforderlich sind. Einige zusätzliche Konfigurationsschritte, die für eine vollständige Konfiguration erforderlich sein können – z. B. für Netzwerkdienste, Geräte-WLAN-Funk, Authentifizierung, SNMP- und Netflow-Einstellungen – werden nicht beschrieben.

Dieses Kapitel enthält die folgenden Themen:

Datencenter-Konfigurationen

Ein SD-WAN Edge in einem Datencenter kann als Hub fungieren, um den Datenverkehr zu bzw. aus den Filialen zu leiten. Der SD-WAN Edge kann verwendet werden, um sowohl MPLS als auch Internetverkehr zu verwalten. Der Hub in einem Datencenter kann in einer ein- oder zweigliedrigen Konfiguration konfiguriert werden. Darüber hinaus kann ein Datencenter als Backup verwendet werden.

Im Folgenden werden die verschiedenen Designs mit verschiedenen Optionen beschrieben, wie SD-WAN Edge in die Topologie eingefügt werden kann.

Option	Beschreibung
Hub 1	Datencenter oder regionale Hub-Site mit einem in einer zweigliedrigen Topologie bereitgestellten SD-WAN Edge.
Hub 2	Datencenter oder regionale Hub-Site mit einem in einer eingliedrigen Topologie bereitgestellten SD-WAN Edge (dieselbe Schnittstelle beinheltet mehrere WAN-Links).
Legacy 1 and 2	Klassische MPLS-Sites.
Silver 1	SD-WAN Edge wird außerhalb des Pfads bereitgestellt. SD-WAN Edge erstellt ein Overlay über MPLS und Internetpfade hinweg. Der Datenverkehr wird zuerst an den SD-WAN Edge umgeleitet.
Silver 2	SD-WAN Edge wird innerhalb des Pfads als Standardgateway bereitgestellt. Er ist immer das Standard-Gateway. Diese Topologie ist einfacher, macht aber SD-WAN Edge zu einer einzelnen Fehlerquelle und kann HA erfordern.
Bronze 1	Dual-Internet-Site (einer der Links befindet sich hinter einem NAT-Router).

Konfigurieren von Zweigstelle und Hub

Dieser Abschnitt bietet einen Überblick über das Konfigurieren von SD-WAN Edge in einer zweigliedrigen Konfiguration.

Übersicht

So konfigurieren Sie den SD-WAN Edge in einer zweigliedrigen Konfiguration:

1 Konfigurieren und Aktivieren von Hub 1

2 Konfigurieren und Aktivieren der Silver 1-Site

3 Aktivieren von Zweigstelle-zu-Hub-Tunnel (Silver 1 bis Hub 1)

4 Konfigurieren und Aktivieren der Bronze 1-Site

5 Konfigurieren und Aktivieren von Hub 2

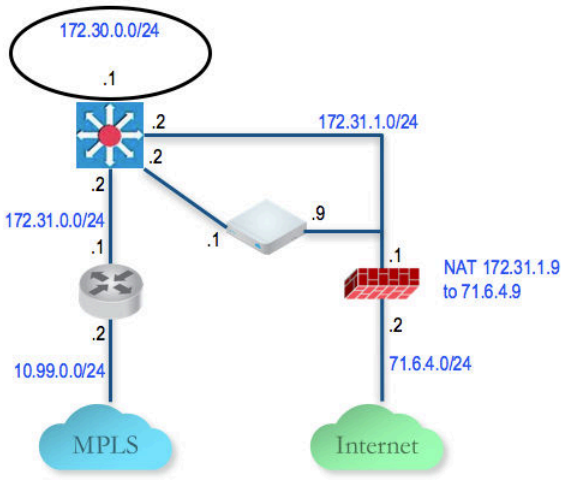
6 Konfigurieren und Aktivieren der Silver 2-Site

In den folgenden Abschnitten werden die Schritte genauer beschrieben.

Konfigurieren und Aktivieren von Hub 1

Mit diesem Schritt können Sie den typischen Workflow zum Ausführen von SD-WAN Edge am Hub-Speicherort verstehen. SD-WAN Edge wird mit zwei Schnittstellen (eine Schnittstelle für jeden WAN-Link) bereitgestellt.

Sie verwenden den virtuellen Edge als Hub. Im Folgenden finden Sie ein Beispiel für die Informationen zur Verkabelung und IP-Adresse.

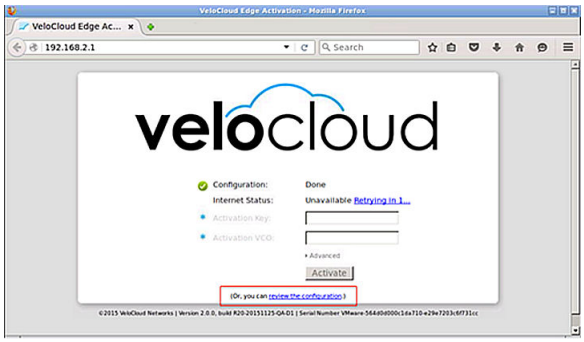


Konfigurieren und Aktivieren des Hub 1-SD-WAN Edge zum Herstellen einer Internetverbindung

Da es sich hierbei um das Datencenter/die Hub-Site handelt, ist es unwahrscheinlich, dass der SD-WAN Edge seine WAN-IP über DHCP abrufen kann. Daher müssen Sie zuerst den SD-WAN Edge aktivieren, um die Internetverbindung über die Firewall des Datencenters herzustellen, damit SD-WAN Edge aktiviert werden kann.

1 Konfigurieren Sie einen PC mit der statischen IP-Adresse **192.168.2.100/24** und dem Gateway **192.168.2.1**. Dies ist die Standard-LAN-Einstellung für den Zugriff auf einen SD-WAN Edge. Verbinden Sie den PC mit der SD-WAN Edge-LAN-Schnittstelle.

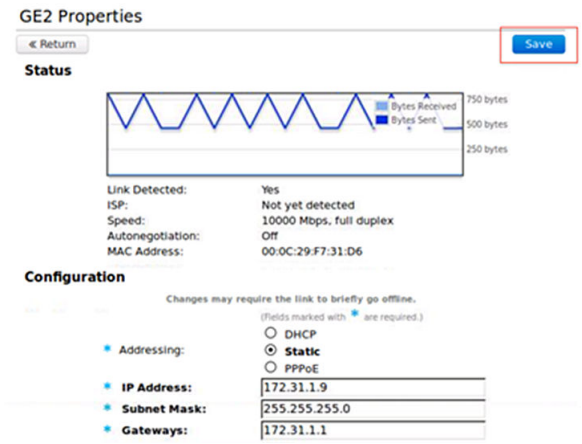
2 Navigieren Sie auf dem PC zu http://192.168.2.1 (die lokale Webschnittstelle des SD-WAN Edge). Klicken Sie auf den Link **Konfiguration überprüfen (review the configuration)**.



3 Konfigurieren Sie die statische WAN-IP von GE2 und das Standardgateway des SD-WAN Edge für den Zugang zum Internet.

Klicken Sie auf **Speichern (Save)** und geben Sie die Anmeldedaten **admin/admin** ein.

Normalerweise wird Ihnen im Datencenter/an der Hub-Site die statische IP-Adresse zugewiesen, und der IT-Administrator des Unternehmens konfiguriert die Firewall so, dass die SD-WAN Edge-WAN-IP in eine öffentliche IP übersetzt und der entsprechende Datenverkehr gefiltert wird (ausgehender Datenverkehr: TCP/443, eingehender Datenverkehr: UDP/2426, UDP/500, UDP/4500).



4 An dieser Stelle sollte der Internetstatus „Verbunden (Connected)“ angezeigt werden.

Nach der Konfiguration der statischen SD-WAN Edge-WAN-IP-Adresse und nach Abschluss der zugehörigen Firewallkonfiguration wird als SD-WAN Edge-Internetstatus „Verbunden (Connected)“ angezeigt.

Aktivieren des virtuellen SD-WAN Edge im Standardprofil

1 Melden Sie sich beim SD-WAN Orchestrator an.

2 Das Standard-VPN-Profil ermöglicht die Aktivierung des SD-WAN Edge 500.

Aktivieren Sie den Hub 1-SD-WAN Edge

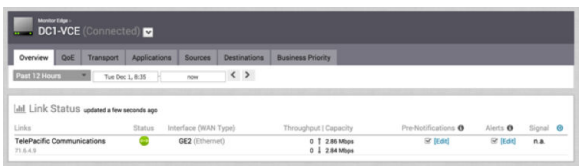
1 Navigieren Sie zu **Konfigurieren (Configure) > Edges** und fügen Sie einen neuen SD-WAN Edge hinzu. Geben Sie das korrekte Modell und das richtige Profil an (wir verwenden das Schnellstart-VPN-Profil).

2 Navigieren Sie zum Hub-SD-WAN Edge (DC1-VCE) und führen Sie die üblichen Aktivierungsschritte aus. Wenn Sie die E-Mail-Funktion bereits eingerichtet haben, wird eine Aktivierungs-E-Mail an diese E-Mail-Adresse gesendet. Anderenfalls können Sie zur Seite „Geräteeinstellung (Device Settings)“ navigieren, um die Aktivierungs-URL zu abzurufen.

3 Kopieren Sie die Aktivierungs-URL und fügen Sie diese in den Browser auf dem PC ein, der mit dem SD-WAN Edge verbunden ist, oder klicken Sie auf die Aktivierungs-URL im Webbrowser.

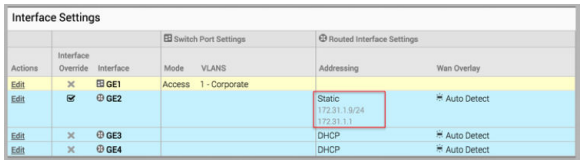
4 Klicken Sie auf die Schaltfläche **Aktivieren (Activate)**.

5 Jetzt sollte der **DC1-VCE**-Datencenter-Hub in Betrieb sein. Navigieren Sie zu **Überwachen (Monitor) > Edges**. Klicken Sie auf die Registerkarte **Edge-Übersicht (Edge Overview)**. Die öffentliche WAN-Link-Kapazität wird zusammen mit der korrekten öffentlichen IP **71.6.4.9** und dem ISP ermittelt.



6 Navigieren Sie zu **Konfigurieren (Configure) > Edges** und wählen Sie **DC1-VCE** aus. Navigieren Sie zur Registerkarte **Gerät (Device)** und scrollen Sie nach unten bis zu den **Schnittstelleneinstellungen (Interface Settings)**.

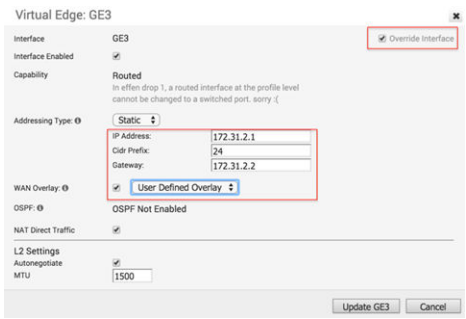
Sie werden feststellen, dass der Registrierungsprozess die SD-WAN Orchestrator-Instanz über die statische WAN-IP-Adresse und das Gateway benachrichtigt, die über die lokale Benutzeroberfläche konfiguriert wurden. Die Konfiguration auf dem VMware SD-WAN wird entsprechend aktualisiert.



7 Scrollen Sie nach unten zum Abschnitt **WAN-Einstellungen (WAN Settings)**. Der Link-Typ sollte automatisch als **Öffentlich verkabelt (Public Wired)** erkannt werden.

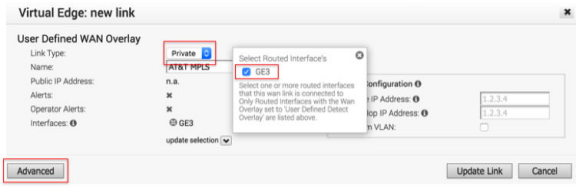
Konfigurieren Sie den privaten WAN-Link auf dem Hub 1-SD-WAN Edge

1 Konfigurieren Sie die private MPLS-Edge-WAN-Schnittstelle direkt über die SD-WAN Orchestrator-Instanz. Navigieren Sie zu **Konfigurieren -> Edges (Configure -> Edges)** und wählen Sie **DC1-VCE** aus. Navigieren Sie zur Registerkarte **Gerät (Device)** und scrollen Sie nach unten bis zum Abschnitt „Schnittstelleneinstellungen (Interface Settings)“. Konfigurieren Sie die statische IP-Adresse auf GE3 als **172.31.2.1/24** und das Standardgateway als **172.31.2.2**. Wählen Sie unter **WAN-Overlay (WAN Overlay)** die Option **Benutzerdefiniertes Overlay (User Defined Overlay)** aus. Dies ermöglicht es uns, im nächsten Schritt manuell einen WAN-Link zu definieren.



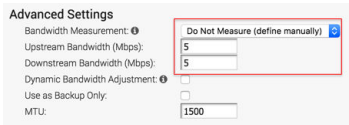
2 Klicken Sie unter **WAN-Einstellungen (WAN Settings)** auf die Schaltfläche **Benutzerdefiniertes WAN-Overlay hinzufügen (Add User Defined WAN Overlay)** (siehe folgende Bildschirmaufnahme).

3 Definieren Sie das WAN-Overlay für den MPLS-Pfad. Wählen Sie den **Link-Typ (Link Type)** als **Privat (Private)** aus und geben Sie die IP-Adresse (172.31.2.2) des WAN-Links im Feld „IP-Adresse (IP Address)“ an. Wählen Sie GE3 als Schnittstelle aus. Klicken Sie auf die Schaltfläche **Erweitert (Advanced)**.



Tipp: Die Hub-Site verfügt normalerweise über mehr Bandbreite als die Zweigstellen. Wenn wir die Bandbreite auswählen, die automatisch ermittelt werden soll, führt die Hub-Site einen Bandbreitentest mit ihrem ersten Peer, z. B. der ersten auftauchenden Zweigstelle, durch und entdeckt am Ende eine falsche WAN-Bandbreite. Für die Hub-Site sollten Sie die WAN-Bandbreite manuell in den erweiterten Einstellungen definieren.

4 Die private WAN-Bandbreite wird in den erweiterte Einstellungen angegeben. Der folgende Screenshot zeigt ein Beispiel von 5 MBit/s vor- und nachgelagerter Bandbreite für einen symmetrischen MPLS-Link am Hub.



5 Prüfen Sie, ob der WAN-Link konfiguriert ist, und speichern Sie die Änderungen.

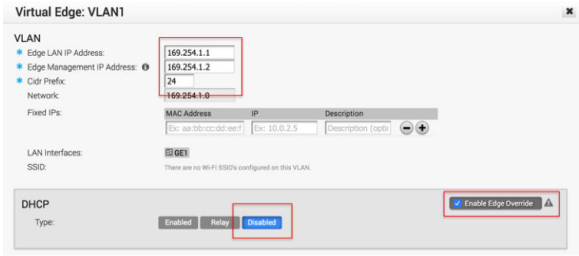
Die Konfiguration des SD-WAN Edge auf dem Hub ist abgeschlossen. Das benutzerdefinierte MPLS-Overlay, das Sie gerade hinzugefügt haben, wird erst angezeigt, wenn Sie einen Zweigstellen-SD-WAN Edge aktivieren.

(Optional) Konfigurieren der LAN-Schnittstelle mit der Verwaltungs-IP

1 Navigieren Sie zu **Konfigurieren (Configure) > Edges** und wählen Sie **DC1-VCE** aus.

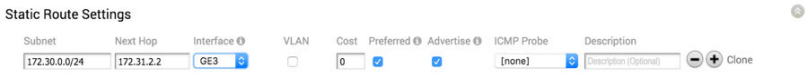
2 Navigieren Sie zur Registerkarte **Gerät (Device)** und scrollen Sie nach unten bis zum Abschnitt „VLAN-Einstellungen (VLAN Settings)“.

3 Klicken Sie auf **Bearbeiten (Edit)** und konfigurieren Sie die IP-Adresse der Schnittstelle.



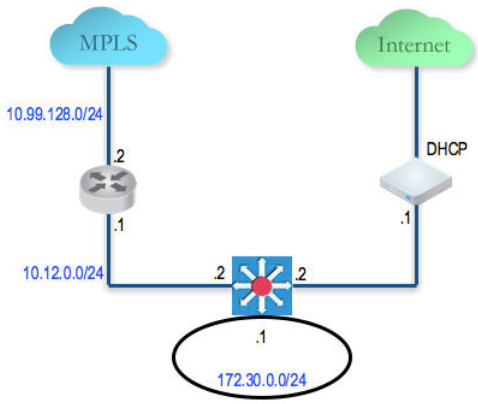
Konfigurieren der statischen Route zum LAN-Netzwerk hinter dem L3-Switch

Fügen Sie eine statische Route zum Subnetz **172.30.0.0 24** über den L3-Switch hinzu. Sie müssen den Schnittstellen-GE3 angeben, der für das Routing zum nächsten Hop verwendet werden soll. Stellen Sie sicher, dass das Kontrollkästchen „Ankündigen (Advertise)“ aktiviert ist, damit ein anderer SD-WAN Edges von diesem Subnetz hinter dem L3-Switch lernen kann (siehe folgende Bildschirmaufnahme).



Konfigurieren und Aktivieren der Silver 1-Site

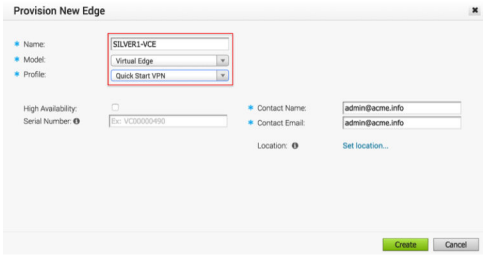
Dieser Schritt hilft Ihnen, den typischen Workflow zum Einfügen des SD-WAN Edge an einer Silver-Site zu verstehen. Der SD-WAN Edge wird außerhalb des Pfads eingefügt und stützt sich auf den L3-Switch, um den Datenverkehr an diesen umzuleiten. Im Folgenden finden Sie ein Beispiel für die Informationen zur Verkabelung und IP-Adresse.



Aktivieren des Zweigstellen-SD-WAN Edge der Silver 1-Site

In diesem Beispiel gehen wir davon aus, dass der SD-WAN Edge seine öffentliche IP-Adresse mithilfe von DHCP erhält, sodass keine Konfiguration erforderlich ist. Im Lieferumfang von SD-WAN Edge ist die Standardkonfiguration zur Verwendung von DHCP auf allen gerouteten Schnittstellen enthalten.

1 Erstellen Sie einen neuen **SILVER1-DCE**-Edge und wählen Sie das entsprechende Modell und Konfigurationsprofil aus (siehe Abbildung unten).



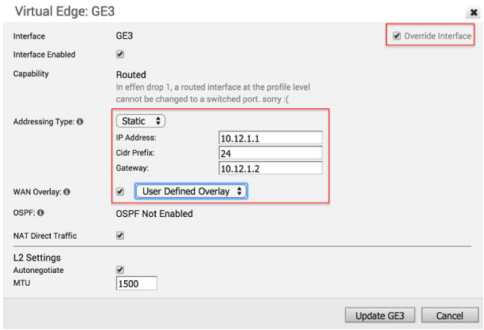
2 Aktivieren Sie diesen SD-WAN Edge, indem Sie einen PC mit seinem LAN oder WLAN verbinden.

3 Der SD-WAN Edge sollte jetzt auf der SD-WAN Orchestrator-Instanz mit einem öffentlichen Link aktiv sein. Jetzt können Sie den privaten WAN-Link konfigurieren.

Konfigurieren des privaten WAN-Link auf dem Silver 1-Site-SD-WAN Edge

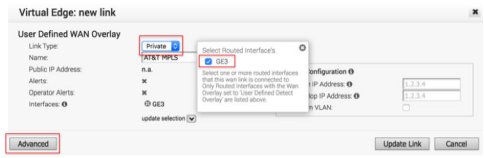
An diesem Punkt müssen wir die IP-Konnektivität vom SD-WAN Edge zum L3-Switch aufbauen.

1 Navigieren Sie zu **Konfigurieren (Configure) > Edges**, wählen Sie den **SILVER1-VCE** aus und navigieren Sie zur Registerkarte „Gerät (Device)“ und scrollen Sie nach unten bis zum Abschnitt „Schnittstelleneinstellungen (Interface Settings)“. Konfigurieren Sie die statische IP-Adresse auf GE3 als **10.12.1.1/24** und das Standardgateway als **10.12.1.2**. Wählen Sie unter **WAN-Overlay (WAN Overlay)** die Option **Benutzerdefiniertes Overlay (User Defined Overlay)** aus. Dies ermöglicht es uns, im nächsten Schritt manuell einen WAN-Link zu definieren.



2 Klicken Sie im Abschnitt **WAN-Einstellungen (WAN Settings)** auf **Benutzerdefiniertes WAN-Overlay hinzufügen (Add User Defined WAN Overlay)**.

3 Definieren Sie das WAN-Overlay für den MPLS-Pfad. Wählen Sie als **Link-Typ (Link Type)** die Option **Privat (Private)** aus. Geben Sie die IP-Adresse (10.12.1.2) des WAN-Links in das IP-Adressfeld ein. Wählen Sie GE3 als Schnittstelle aus. Klicken Sie auf die Schaltfläche **Erweitert (Advanced)**.



Tipp: Da der Hub bereits eingerichtet wurde, ist es in Ordnung, die Bandbreite automatisch zu ermitteln. Diese Zweigstelle führt einen Bandbreitentest mit dem Hub aus, um dessen Link-Bandbreite zu ermitteln.

4 Legen Sie für die Bandbreitenmessung **Bandbreite messen (Measure Bandwidth)** fest. Dies führt dazu, dass der Zweigstellen-SD-WAN Edge einen Bandbreitentest mit dem Hub-SD-WAN Edge ausführt, genau wie beim Verbindungsaufbau zum SD-WAN Gateway.

5 Bestätigen Sie, dass der WAN-Link konfiguriert ist, und speichern Sie die Änderungen (siehe folgende Bildschirmaufnahme).

(Optional) Konfigurieren der LAN-Schnittstelle mit der Verwaltungs-IP

1 Navigieren Sie zu **Konfigurieren (Configure) > Edges** und wählen Sie **SILVER1-VCE** aus. Navigieren Sie zur Registerkarte **Gerät (Device)** und scrollen Sie nach unten bis zum Abschnitt „VLAN-Einstellungen (VLAN Settings)“. Klicken Sie auf **Bearbeiten (Edit)**. Konfigurieren Sie die IP-Adresse des LAN und der Verwaltungsschnittstellen.

Konfigurieren der statischen Route zum LAN-Netzwerk hinter dem L3-Switch

Fügen Sie eine statische Route zu **192.168.128.0/24** über den L3-Switch hinzu. Sie müssen den Schnittstellen-GE3 angeben. Stellen Sie sicher, dass das Kontrollkästchen „Ankündigen (Advertise)“ aktiviert ist, damit ein anderer SD-WAN Edges von diesem Subnetz hinter dem L3-Switch lernen kann (siehe folgende Bildschirmaufnahme).

Aktivieren von Zweigstelle-zu-Hub-Tunnel (Silver 1 bis Hub 1)

Mit diesem Schritt können Sie den Overlay-Tunnel aus der Zweigstelle in den Hub erstellen. Beachten Sie, dass Sie an diesem Punkt zwar sehen können, dass der Link aktiv ist, aber dies ist der Tunnel zum SD-WAN Gateway über den Internetpfad und nicht der Tunnel zum Hub. Wir müssen Cloud-VPN aktivieren, um zu ermöglichen, dass der Tunnel von der Zweigstelle zum Hub hergestellt werden kann.

Der Tunnel von der Zweigstelle zum Hub kann jetzt erstellt werden.

Aktivieren von Cloud-VPN und Edge-zu-SD-WAN Hub-Tunnel

1 Schritt 1: Navigieren Sie zu **Konfigurieren (Configure)** > **Profile (Profiles)**, wählen Sie **Schnellstart-VPN-Profil (Quick Start VPN Profile)** aus und navigieren Sie zur Registerkarte **Gerät (Device)**. Aktivieren Sie das Cloud-VPN und führen Sie die folgenden Schritte aus.

   - Aktivieren Sie unter **Zweigstelle-zu-Hubs (Branch to Hubs)** das Kontrollkästchen **Aktivieren (Enable)**.
   - Aktivieren Sie unter **Zweigstelle-zu-Zweigstelle-VPN (Branch to Branch VPN)** das Kontrollkästchen **Aktivieren (Enable)**.
   - Aktivieren Sie unter **Zweigstelle-zu-Zweigstelle-VPN (Branch to Branch VPN)** das Kontrollkästchen „Cloud-Gateways verwenden (Use Cloud Gateways)“. Auf diese Weise wird die Datenebene durch das SD-WAN Gateway für Zweigstelle-zu-Hub-VPN deaktiviert. Der Zweigstelle-zu-Zweigstelle-Datenverkehr durchläuft zunächst einen der Hubs (in der geordneten Liste, die Sie als Nächstes angeben), während der direkte Zweigstelle-zu-Zweigstelle-Tunnel eingerichtet wird.

   Klicken Sie auf **Hubs auswählen (Select Hubs)**. Verschieben Sie den **DC1-VCE** dann nach rechts. Hiermit wird der **DC1-VCE** als SD-WAN Hub bezeichnet. Klicken Sie auf **DC1-VCE** in den Hubs und klicken Sie auf die Schaltflächen **Backhaul-Hubs aktivieren (Enable Backhaul Hubs)** und **B2B-VPN-Hubs aktivieren (Enable B2B VPN Hubs)**. Sie verwenden denselben **DC1-VCE** für den Zweigstelle-zu-Zweigstelle-Datenverkehr und für den Backhaul-Internet-Datenverkehr zum Hub. Im Abschnitt „Cloud-VPN (Cloud VPN)“ wird **DC1-VCE** sowohl als SD-WAN Hubs angezeigt als auch für die Verwendung für Zweigstelle-zu-Zweigstelle-VPN-Hubs.

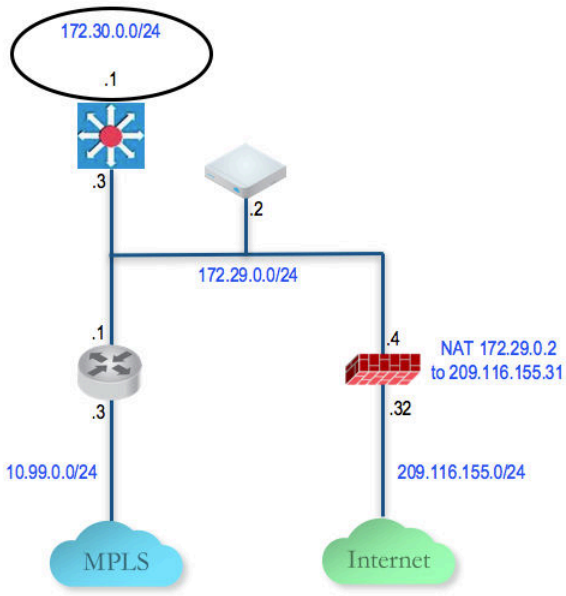
2 Zu diesem Zeitpunkt sollte der direkte Tunnel zwischen der Zweigstelle und dem Hub-SD-WAN Edges verfügbar sein. Mit dem Debugging-Befehl wird nun auch der direkte Tunnel zwischen der Zweigstelle und dem Hub angezeigt. Das folgende Beispiel stammt aus dem **SILVER1-VCE**. Beachten Sie die zusätzlichen Tunnel zu **71.6.4.9** und **172.31.2.1**. Hierbei handelt es sich um die direkten Tunnel zum Hub-SD-WAN Edge (GE2 über öffentliches Internet und GE3 über den privaten Link).

Konfigurieren und Aktivieren der Bronze 1-Site

Dieser Schritt hilft bei der Erstellung einer Bronze-Site — einer dualen Internet-Site mit einer DIA und einem Breitbandanschluss. Im Folgenden finden Sie ein Beispiel für die Informationen zur Verkabelung und IP-Adresse. Das SD-WAN Edge-LAN namens **BRONZE1-VCE** und die Aktivierung des SD-WAN Edge. Es ist keine Konfiguration für das WAN erforderlich, da es DHCP für beide WAN-Schnittstellen verwendet.

Konfigurieren und Aktivieren von Hub 2

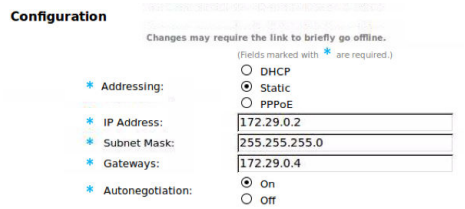
Mit diesem Schritt können Sie die „Lenkung über IP-Adresse“-Einstellung konfigurieren, die in zweigliedrigen Hub-Bereitstellungen häufig verwendet wird. Im Folgenden finden Sie ein Beispiel für die Informationen zur Verkabelung und IP-Adresse. Mit einer eingliedrigen Bereitstellung kann dieselbe Tunnelquell-IP-Adresse verwendet werden, um ein Overlay über verschiedene Pfade zu erstellen.



Konfigurieren Sie den Hub 2-SD-WAN Edge zum Herstellen einer Internetverbindung.

1 Verbinden Sie einen PC mit dem SD-WAN Edge und geben Sie im Browser http://192.168.2.1 ein.

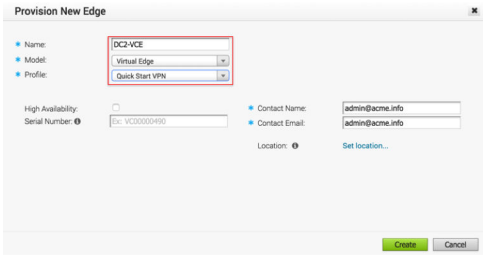
2 Konfigurieren Sie den Hub-SD-WAN Edge zum Herstellen einer Internetverbindung, indem Sie die erste WAN-Schnittstelle (GE2) konfigurieren.



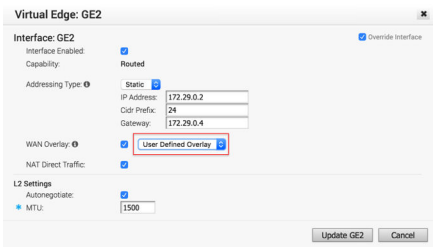
Fügen Sie den Hub 2-SD-WAN Edge zur SD-WAN Orchestrator-Instanz hinzu und aktivieren Sie ihn.

In diesem Schritt erstellen Sie den zweiten Hub-SD-WAN Edge, der als **DC2.VCE** bezeichnet wird.

1 Navigieren Sie in SD-WAN Orchestrator zu **Konfigurieren (Configure)** > **Edges** und wählen Sie **Neuer Edge (New Edge)** aus, um einen neuen SD-WAN Edge hinzuzufügen.



2 Navigieren Sie zu **Konfigurieren (Configure)** > **Edges**, wählen Sie den SD-WAN Edge aus, den Sie gerade erstellt haben, und klicken Sie dann auf die Registerkarte **Gerät (Device)**, um dieselbe Schnittstelle und IP-Adresse zu konfigurieren, die Sie im vorherigen Schritt konfiguriert haben.

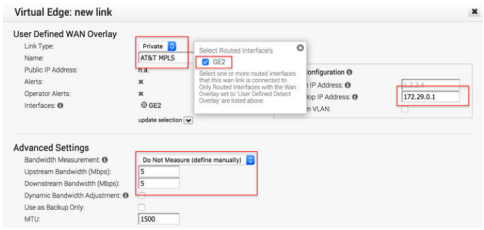


Wichtig Da wir den SD-WAN Edge im eingliedrigen Modus einsetzen (gleiche physische Schnittstelle, aber von dieser Schnittstelle aus gibt es mehrere Übertunnel), ist es wichtig, das WAN-Overlay als benutzerdefiniert festzulegen.

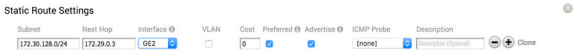
3 An dieser Stelle müssen Sie das Overlay erstellen. Klicken Sie unter **WAN-Einstellungen (WAN Settings)** auf **Benutzerdefiniertes WAN-Overlay hinzufügen (Add User Defined WAN Overlay)**.

4 Erstellen Sie ein Overlay über den öffentlichen Link hinweg. In diesem Beispiel verwenden Sie für den nächsten Hop die IP-Adresse **172.29.0.4**, um das Internet über die Firewall zu erreichen. Die Firewall ist bereits für die NAT-Weiterleitung des Datenverkehrs an **209.116.155.31** konfiguriert.

5 Fügen Sie das zweite Overlay über das private Netzwerk hinzu. In diesem Beispiel geben Sie **172.29.0.1** als Router für den nächsten Hop an und legen die Bandbreite fest, da es sich um den MPLS-Abschnitt handelt und **DC2-VCE** ein Hub ist.



Fügen Sie eine statische Route zum LAN-seitigen Subnetz **172.30.128.0/24** über GE2 hinzu (siehe folgende Bildschirmaufnahme).



6 Aktivieren Sie den SD-WAN Edge. Nachdem die Aktivierung erfolgreich war, kehren Sie zur Registerkarte **Gerät (Device)** unter der Konfiguration auf Edge-Ebene zurück. Beachten Sie, dass das Feld „Öffentliche IP (Public IP)“ jetzt ausgefüllt ist. Sie sollten nun die Links in **Überwachen (Monitor) > Edges** unter der Registerkarte **Übersicht (Overview)** sehen. **(Optional) Konfigurieren der LAN-Schnittstelle mit der Verwaltungs-IP**Navigieren Sie zu **Konfigurieren (Configure) > Edges** und wählen Sie **DC2-VCE** aus. Navigieren Sie zur Registerkarte **Gerät (Device)** und scrollen Sie nach unten bis zum Abschnitt „VLAN-Einstellungen (VLAN Settings)“. Klicken Sie auf **Bearbeiten (Edit)**. Konfigurieren Sie die IP-Adresse des LAN und der Verwaltungsschnittstellen.

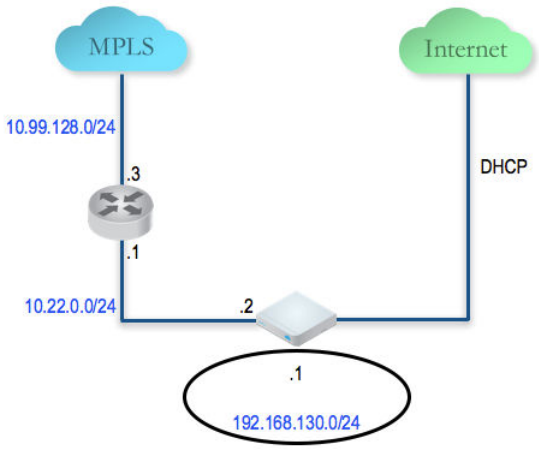
Hinzufügen des Hub 2-SD-WAN Edge zur Hub-Liste im Schnellstart-VPN-Profil

1 Navigieren Sie zu **Konfigurieren (Configure) > Profile (Profiles)** und wählen Sie das Profil **Schnellstart-VPN (Quick Start VPN)** aus.

2 Navigieren Sie zur Registerkarte **Gerät (Device)** und fügen Sie diesen neuen SD-WAN Edge zu einer Liste von Hubs hinzu.

Konfigurieren und Aktivieren der Silver 2-Site

Dieser Schritt hilft Ihnen bei der Erstellung einer Silver-Site (einer hybriden Site), bei der sich der SD-WAN Edge hinter dem CE-Router befindet und bei dem SD-WAN Edge der Standardrouter für das LAN ist. Nachstehend finden Sie ein Beispiel für die Verkabelung und die IP-Adressinformationen für jede Hardware.



Verbinden Sie einen PC mit dem SD-WAN Edge-LAN oder -WLAN und geben Sie im Browser http://192.168.2.1 ein.

Konfigurieren von dynamischem Routing mit OSPF oder BGP

19

In diesem Abschnitt wird beschrieben, wie Sie dynamisches Routing mit OSPF oder BGP konfigurieren.

SD-WAN Edge lernt Routen von benachbarten Routern über OSPF und BGP. Er sendet die gelernten Routen an das Gateway/den Controller. Das Gateway bzw. der Controller fungiert wie ein Routenreflektor und sendet die erlernten Routen an andere SD-WAN Edges. Die OFC (Overlay Flow Control, Overlay-Flow-Steuerung) ermöglicht eine unternehmensweite Routensichtbarkeit und -steuerung für eine einfache Programmierung und für Voll- oder Teil-Overlay.

VMware SD-WAN unterstützt Eingangs-/Ausgangsfilter zu OSPF-Nachbarn, OE1/OE2-Routentypen, MD5-Authentifizierung. Über OSPF gelernte Routen werden automatisch an den in der Cloud oder an die lokal gehosteten Controller weiterverteilt. Unterstützung für BGP-Eingangs-/Ausgangsfilter, und der Filter kann auf „Verweigern (Deny)“ festgelegt werden. Optional können Sie das BGP-Attribut hinzufügen/ändern, um die Pfadauswahl zu beeinflussen, d. h. RFC 1998-Community, MED und lokale Präferenz.

Hinweis Weitere Informationen zur OSPF- und BGP-Neuverteilung finden Sie im Abschnitt mit dem Titel OSPF/BGP-Umverteilung.

Hinweis In der Version 3.2 können sowohl BGP als auch OSPF gleichzeitig auf einem SD-WAN Edge aktiviert werden.

Dieses Kapitel enthält die folgenden Themen:

- Aktivieren von OSPF
- BGP aktivieren
- OSPF/BGP-Umverteilung
- Overlay-Flow-Steuerung

Aktivieren von OSPF

OSPF (Open Shortest Path First) kann ausschließlich auf der LAN-Schnittstelle als passive Schnittstelle aktiviert werden. Der Edge kündigt nur das Präfix an, das mit dem LAN-Switch-Port

verknüpft ist. Für vollen Funktionsumfang müssen Sie OSPF in gerouteten Schnittstellen verwenden.

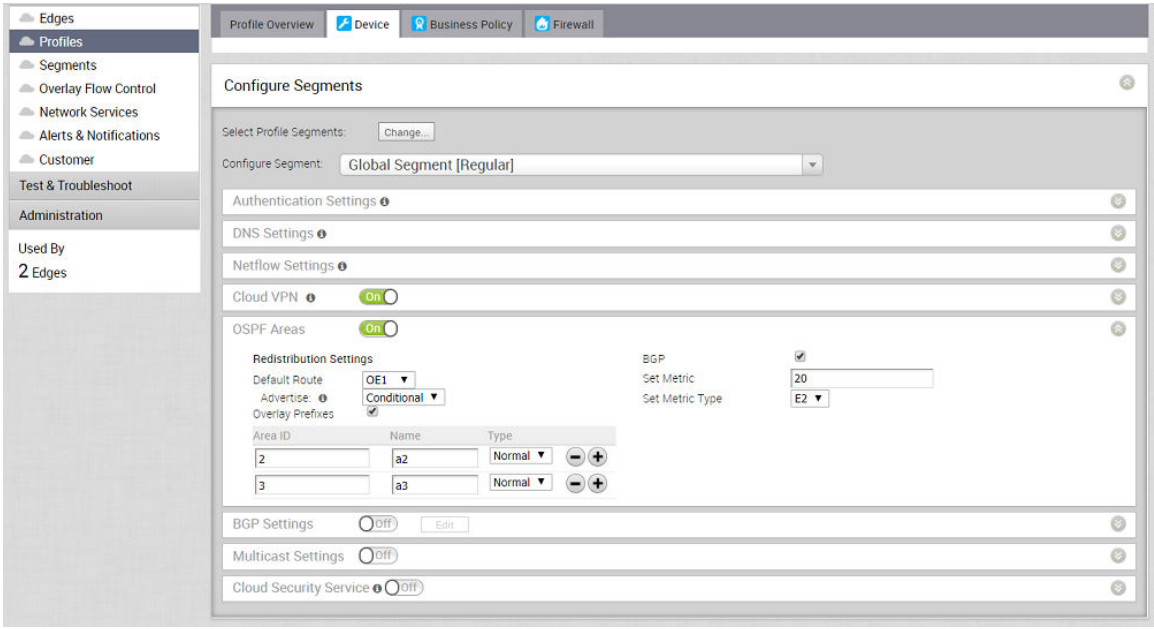
Führen Sie zum Aktivieren von OSPF die Schritte in diesem Verfahren durch:

1 Konfigurieren Sie OSPF für VPN-Profile.

a Navigieren Sie zu **Konfigurieren (Configure) > Profil (Profile)**.

b Klicken Sie auf das Symbol **Gerät (Device)** für das VPN-Profil, für das OSPF konfiguriert werden soll.

Der Bildschirm **Segmente konfigurieren (Configure Segments)** wird angezeigt.



c Setzen Sie im Abschnitt **OSPF-Bereiche (OSPF Areas)** die Umschaltfläche **OSPF-Bereiche (OSPF Areas)** auf **EIN (ON)**.

d Konfigurieren Sie die Neuverteilungseinstellungen für OSPF-Bereiche.

1 Wählen Sie im Dropdown-Menü **Standardroute (Default Route)** einen als Standardroute zu verwendenden OSPF-Routentyp (E1 oder E2) aus.

2 Wählen Sie im Dropdown-Menü **Ankündigen (Advertise)** die Option **Immer (Always)** oder **Bedingt (Conditional)** aus. (Bei Auswahl von „Immer (Always)“ wird die Standardroute immer angekündigt. Bei Auswahl von „Bedingt (Conditional)“ wird die Standardroute nur dann neu verteilt, wenn der Edge Routen über Overlay oder Underlay erlernt.) Die Option „Overlay-Präfixe (Overlay Prefixes)“ muss zur Verwendung der bedingten Standardroute aktiviert werden.

3 Aktivieren Sie gegebenenfalls das Kontrollkästchen **Overlay-Präfixe (Overlay Prefixes)**.

4 Zum Aktivieren der Einfügung von BGP-Routen in OSPF aktivieren Sie optional das Kontrollkästchen **BGP**. BGP-Routen können in OSPF neu verteilt werden. Wenn dies zutrifft, geben Sie die Konfigurationsoptionen ein oder wählen Sie sie wie folgt aus:

   a Geben Sie im Textfeld **Metrik festlegen (Set Metric)** die Metrik ein. (Hierbei handelt es sich um die Metrik, die OSPF in den zugehörigen externen LSAs festlegt, die anhand der neu verteilten Routen erzeugt werden.) Die Standardmetrik lautet 20.

   b Wählen Sie im Dropdown-Menü **Metriktyp festlegen (Set Metric Type)** einen Metriktyp aus. (Hierbei handelt es sich entweder um den Typ E1 oder E2 (externer LSA-Typ von OSPF); der Standardtyp ist E2.)

5 Geben Sie im Textfeld **ID** eine **OSPF-Bereichs-ID (OSPF Area ID)** ein.

6 Geben Sie im Textfeld **Name** einen beschreibenden Namen für den Bereich ein.

7 Standardmäßig ist der Typ **Normal** ausgewählt. Aktuell wird nur der Typ **Normal** unterstützt.

8 Fügen Sie gegebenenfalls weitere Bereiche hinzu, indem Sie auf klicken.

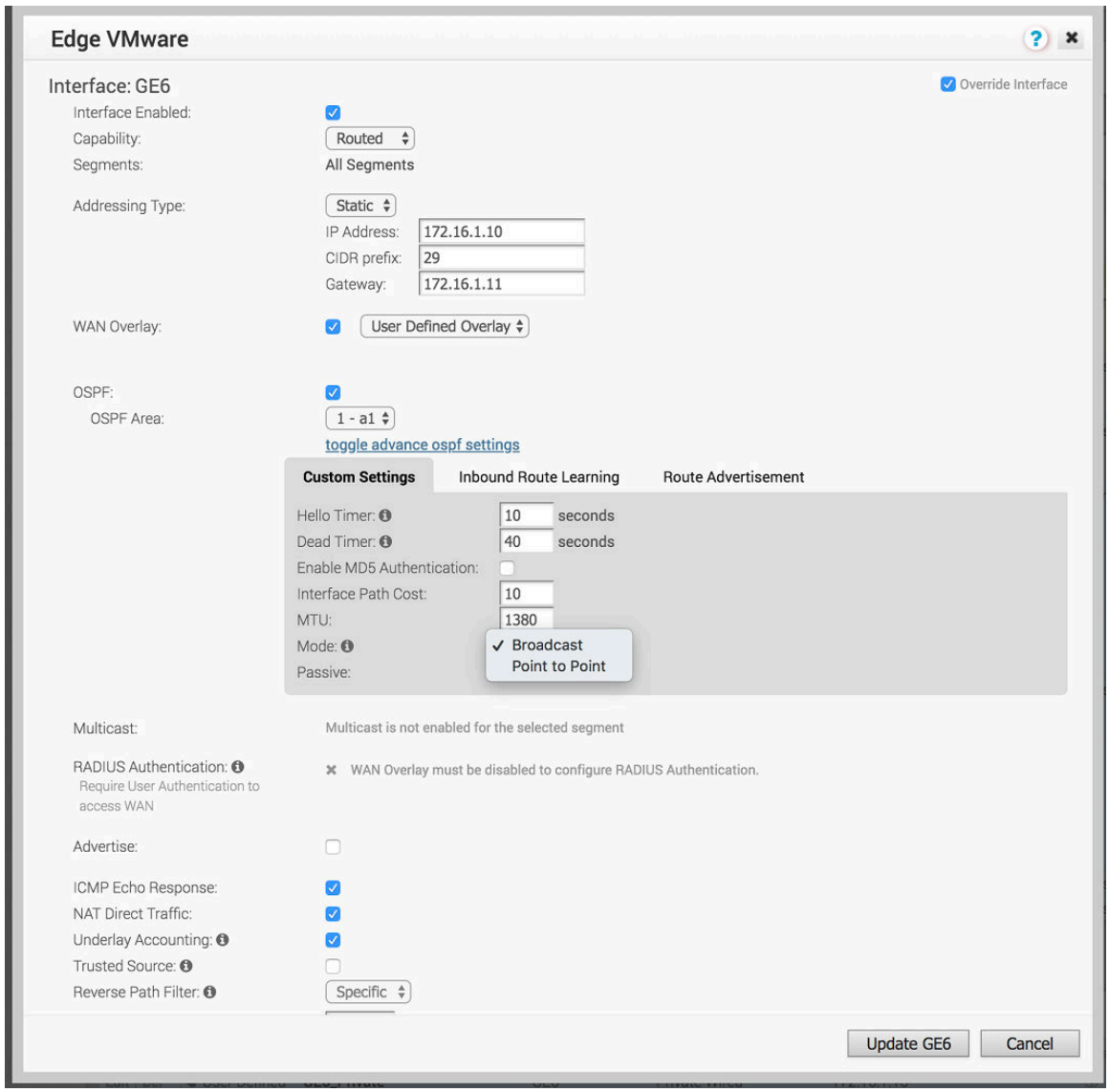
2 Konfigurieren Sie geroutete Schnittstelleneinstellungen für das OSPF-fähige Edge-Gerät.

Hinweis SD-WAN Orchestrator unterstützt den OSPF-Netzwerkmodus **Punkt-zu-Punkt (Point to Point)** auf Edge- und Profilebene.

a Führen Sie im Bildschirm **Segmente konfigurieren (Configure Segments)** einen Bildlauf zum Bereich **Geräteeinstellungen (Device Settings)** des Edge-Geräts durch, für das Schnittstellen- und OSPF-Einstellungen konfiguriert werden sollen.

b Klicken Sie auf das Symbol zum Erweitern, das dem Edge entspricht.

c Klicken Sie im Bereich **Schnittstelleneinstellungen (Interface Settings)** auf den Link **Bearbeiten (Edit)** der Schnittstelle. Der Bildschirm „Schnittstelleneinstellung (Interface Setting)“ für das Edge-Gerät wird angezeigt.



d Aktivieren Sie das Kontrollkästchen **OSPF**.

e Wählen Sie im Dropdown-Menü **OSPF-Bereich (OSPF Area)** einen OSPF-Bereich aus.

f Klicken Sie auf den Link **Erweiterte OSPF-Einstellungen umschalten (Toggle Advanced OSPF Settings)**, um erweiterte OSPF-Einstellungen zu konfigurieren.

1 Erstellen Sie Filter für **Erlernen eingehender Routen (Inbound Route Learning)** und **Routenankündigung (Route Advertisement)**. Weitere Informationen finden Sie unter Routenfilter.

2 Klicken Sie auf die Registerkarte **Benutzerdefinierte Einstellungen (Custom Settings)** und konfigurieren Sie die folgenden OSPF-Einstellungen.

a Geben Sie im Textfeld **Hello-Timer (Hello Timer)** das Intervall für den OSPF-Hello-Timer in Sekunden ein. Der zulässige Bereich liegt zwischen 1 und 255.

b Geben Sie im Textfeld **Dead-Timer (Dead Timer)** das Intervall für den OSPF-Dead-Timer in Sekunden ein. Der zulässige Bereich liegt zwischen 1 und 65535.

c Aktivieren Sie das Kontrollkästchen **MD5-Authentifizierung aktivieren (Enable MD5 Authentication)**, um MD5-Authentifizierung zu aktivieren.

d Geben Sie im Textfeld **Kosten für Schnittstellenpfad (Interface Path Cost)** die OSPF-Kosten für den Schnittstellenpfad ein.

e Geben Sie im Textfeld **MTU** den Wert für die maximale Übertragungseinheit (Maximum Transmission Unit, MTU) der Schnittstelle ein.

f Wählen Sie im Dropdown-Menü **Modus (Mode)** als Modus für den OSPF-Netzwerktyp entweder **Broadcast** oder **Punkt-zu-Punkt (Point to Point)** aus. Der Standardmodus für OSPF lautet **Broadcast**.

g Aktivieren Sie das Kontrollkästchen **Passiv (Passive)**, um den passiven OSPF-Modus zu aktivieren.

h Klicken Sie auf die Schaltfläche **Aktualisieren (Update)**.

3 Klicken Sie auf **Änderungen speichern (Save Changes)**.

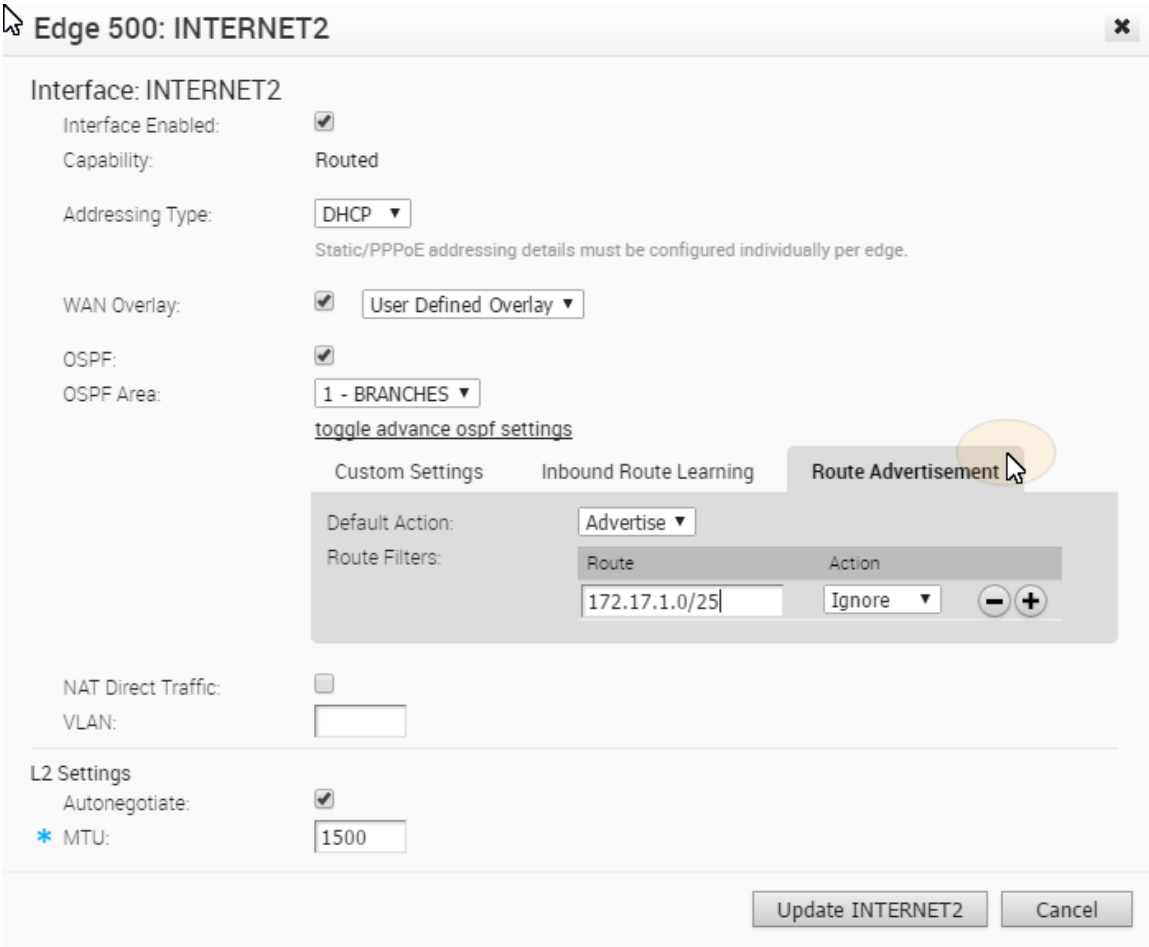
Im angezeigten Dialogfeld **Änderungen bestätigen (Confirm Changes)** werden Sie aufgefordert, die zu aktivierenden OSPF-Bereiche zu bestätigen. Außerdem wird die Anzahl der betroffenen Edges angezeigt.

Hinweis Bei Edges, die nicht mit der OSPF-Konfiguration auf Profilebene verknüpft sind, müssen Sie eine Konfiguration auf Edge-Ebene über **Konfigurieren (Configure) > Edges > Gerät (Device) > Bereich „Schnittstelleneinstellungen (Interface Settings)“** durchführen.

Routenfilter

Es gibt zwei verschiedene Arten von Routing: Eingangsrouting und Ausgangsrouting.

- Eingangsrouting umfasst Einstellungen, die von OSPF gelernt oder ignoriert und in der Overlay-Flow-Steuerung installiert werden können.
- Ausgangsrouting gibt an, welche Präfixe in OSPF umverteilt werden können.



BGP aktivieren

Auf Enterprise-Ebene ist die Funktion „Routing-BGP (Routing BGP)“ standardmäßig aktiviert. Sie können BGP pro Segment konfigurieren, indem Sie die Schritte in diesem Verfahren ausführen.

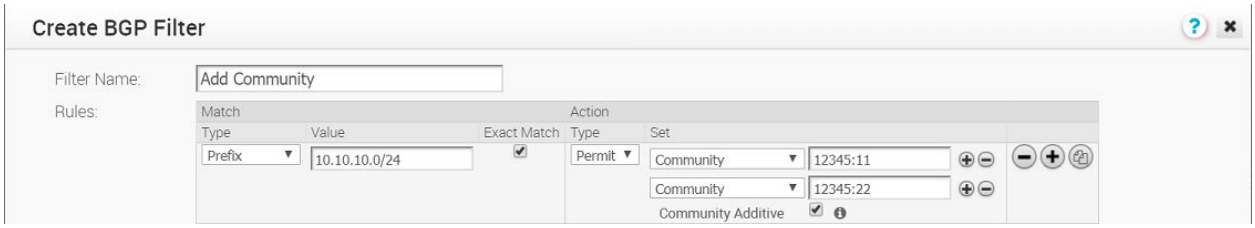
Hinweis

- 4-Byte-ASN-BGP wird unterstützt, Peer zu einem Nachbarn mit 4-Byte-ASN- 4-Byte-ASNs in Routenankündigungen akzeptieren. Nur einfaches Format wird unterstützt. Das asdot/ Dezimalformat wird nicht unterstützt.
- BGP kann pro Segment konfiguriert werden. Konfigurationen sind auf der Profil- oder Edge-Ebene mit aktivierter Edge-Überschreibung möglich.

Unterstützung für Community-Additif (Community Additive Support)

Die eingehende und ausgehende BGP-Konfiguration unterstützt die Einrichtung von BGP-Communitys. Community-Werte können verwendet werden, um die Quelle der Routen anzugeben. Wenn „Additif (Additive)“ nicht aktiviert ist, wird die vorhandene BGP-Community standardmäßig durch die „festgelegten“ Werte ersetzt. Wenn die Option „Community-Additif

(Community Additive)“ aktiviert ist, werden die festgelegten Community-Werte zur vorhandenen BGP-Community hinzugefügt. Wie in folgender Beispielabbildung dargestellt, werden Community 12345:11 und 12345:22 an die vorhandene BGP-Community angehängt. Hinweis: Die maximale Anzahl der unterstützten Community-Zeichenfolgen beträgt zwölf.



1 Konfigurieren von BGP für VPN-Profile:

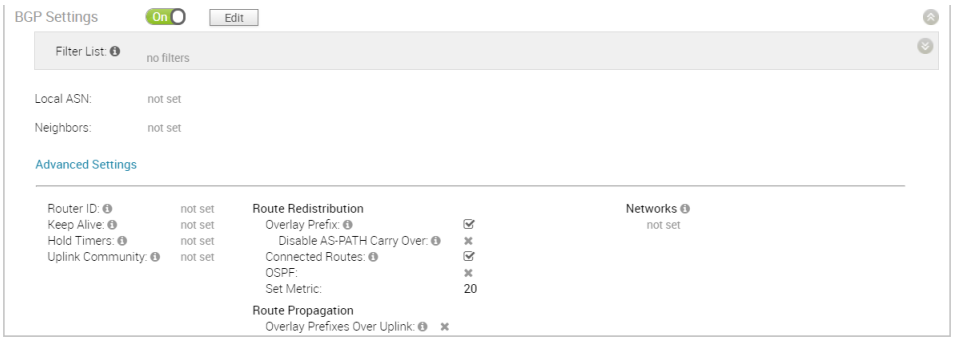
   a Wechseln Sie im Navigationsbereich zu **Konfigurieren (Configure) > Profil (Profile)**.

   Der Bildschirm **Konfigurationsprofile (Configuration Profiles)** wird angezeigt.

   b Wählen Sie ein Profil aus, für das BGP aktiviert werden soll, und klicken Sie für das anwendbare Profil auf das Symbol **Gerät (Device)**.

   Der Bildschirm **Geräteeinstellungen (Device Settings)** für das ausgewählte Profil wird angezeigt.

2 Führen Sie einen Bildlauf nach unten zum Bereich **BGP-Einstellungen (BGP Settings)** durch und aktivieren Sie **BGP EIN (BGP ON)** (siehe folgende Abbildung).

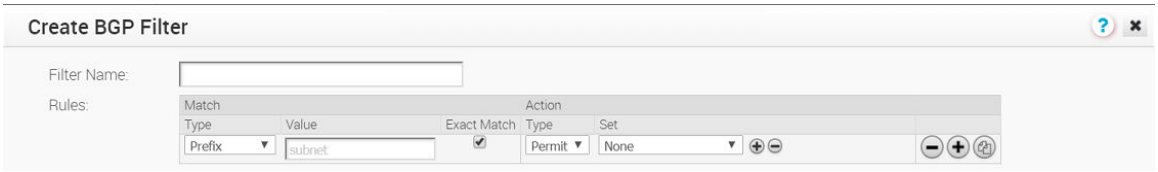


3 Klicken Sie auf die Schaltfläche **Bearbeiten (Edit)**, um die BGP-Nachbarn zu definieren.

4 Führen Sie im **BGP-Editor (BGP Editor)** folgende Schritte durch:

   a Klicken Sie auf die Schaltfläche **Filter hinzufügen (Add Filter)**, um einen oder mehrere Filter zu erstellen. (Diese Filter werden auf den Nachbarn angewendet, um die Attribute der Route abzulehnen oder zu ändern. Derselbe Filter kann für mehrere Nachbarn verwendet werden).

   Das Dialogfeld **BGP-Filter erstellen (Create BGP Filter)** wird angezeigt (Abbildung unten).



b Führen Sie im Dialogfeld **BGP-Filter erstellen (Create BGP Filter)** folgende Schritte durch:

1 Geben Sie im Textfeld **Filtername (Filter Name)** einen Namen für den Filter ein.

2 Legen Sie die Regeln für den Filter fest.

- Wählen Sie im Dropdown-Menü **Typ (Type)** die Option „Präfix (Prefix)“ oder „Community“ aus.
- Legen Sie den Wert für das Präfix oder die Community im Textfeld **Wert (Value)** fest.
- Aktivieren Sie gegebenenfalls das Kontrollkästchen **Genaue Übereinstimmung (Exact Match)**.
- Geben Sie den Aktionstyp (Zulassen (Permit) oder Ablehnen (Deny)) aus dem Dropdown-Menü **Typ (Type)** an.
- Aktivieren Sie im Dropdown-Menü **Festlegen (Set)** das Kontrollkästchen „Keine (None)“, „Lokale Präferenz (Local Preference)“, „Metrik (Metric)“, „AS-Pfad voranstellen (AS-Path-Prepend)“ „Community“ oder „Community-Additif (Community Additive)“. Weitere Informationen finden Sie im obigen Abschnitt mit dem Titel Unterstützung für Community-Additif.

Eine Beschreibung dieser Felder finden Sie in der folgenden Tabelle (die Abbildung unterhalb der Tabelle dient als Referenz).

Regelfeld	Beschreibung
Übereinstimmungstyp (Match Type): Präfix (Prefix) oder Community	
Wert (Value)	
Kontrollkästchen „Genaue Übereinstimmung (Exact Match)“	
Aktionstyp (Action Type): Zulassen (Permit) oder Ablehnen (Deny)	
Option „Festlegen (Set)“: Keine (None)	
Option „Festlegen (Set)“: Lokale Präferenz (Local Preference)	

Regelfeld	Beschreibung
Option „Festlegen (Set)“: Kontrollkästchen „Community“ und „Community-Additif (Community Additive)“.	Die eingehende und ausgehende BGP-Konfiguration unterstützt die additive Konfigurationsoption. Hiermit werden eingehende Community-Attribute und Setup-Community-Werte angehängt. Community-Werte können verwendet werden, um die Quelle der Routen anzugeben. Wenn „Additif (Additive)“ nicht aktiviert ist, wird der Community-Wert standardmäßig durch den „festgelegten“ Wert ersetzt.
Option „Festlegen (Set)“: Metrik (Metric)	
Option „Festlegen (Set)“: AS-Pfad anhängen (AS-Path-Prepend)	

c Klicken Sie nach dem Festlegen der Regeln für den Filter auf die Schaltfläche **OK**.

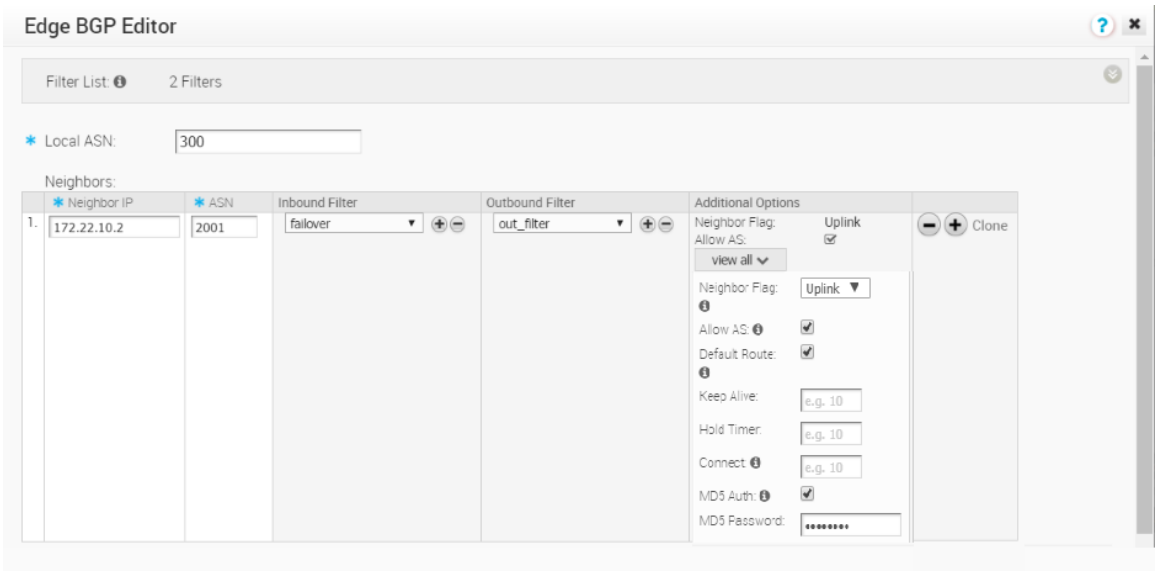
d Geben Sie im Dialogfeld **BGP-Editor (BGP-Editor)** die lokale ASN-Nummer im Textfeld **Lokale ASN (Local ASN)** ein.

e Geben Sie im Bereich „Nachbar (Neighbor)“ die **Nachbar-IP (Neighbor IP)** und **ASN** in den entsprechenden Textfeldern ein und legen Sie die eingehenden und ausgehenden Filter aus der im vorherigen Schritt definierten Liste **Filter** fest.

f Fügen Sie zusätzliche Optionen hinzu, indem Sie auf die Schaltfläche **Alle anzeigen (View All)** klicken, um das Dropdown-Menü zu öffnen. Wenden Sie gegebenenfalls zusätzliche Optionen an. (Die folgende Tabelle enthält eine Beschreibung der einzelnen Optionen und dient zu Referenzzwecken.)

Feld „Zusätzliche Optionen (Additional Options)“	Beschreibung
Dropdown-Menü „Nachbar-Flag (Neighbor Flag)“	Wird verwendet, um den Nachbartyp zu kennzeichnen. Im Dropdown-Menü stehen zwei Optionen zur Auswahl: „Keiner (None)“ und Uplink. Wählen Sie „Uplink“ aus, wenn er als WAN-Overlay für MPLS verwendet wird. Diese Option wird als Flag verwendet, um zu entscheiden, ob die Site als Transit-Site (z. B. Hub) fungieren soll, indem über SD-WAN-Overlay erlernte Routen an WAN-Links für MPLS weitergegeben werden. Wenn eine Transit-Site benötigt wird, aktivieren Sie „Overlay-Präfix über Uplink (Overlay Prefix Over Uplink)“ in der Option „Erweitert (Advanced)“.
Kontrollkästchen „AS zulassen (Allow AS)“	Erlernen der BGP-Routen, obwohl sich dasselbe AS im AS-Pfad befindet.
Kontrollkästchen „Standardroute (Default Route)“	Ankündigen einer Standardroute zum Nachbarn. Weitere Informationen zur Verwendung des Kontrollkästchens **Standardroute (Default Route)** finden Sie im Schritt „e, ii“ weiter unten.

Feld „Zusätzliche Optionen (Additional Options)“	Beschreibung
Verbinden (Connect)	Intervall in Sekunden, bevor eine neue TCP-Verbindung mit dem Peer hergestellt wird, wenn erkannt wird, dass die TCP-Sitzung nicht passiv ist. Der Standardwert beträgt 120 Sekunden.
Kontrollkästchen „MD5-Authentifizierung (MD5 Auth)“	Aktiviert die BGP-MD5-Authentifizierung. Das Kontrollkästchen „MD5-Authentifizierung (MD5 Auth)“ wird in einem Legacy- oder Verbundnetzwerk verwendet. Generell wird BGP-MD5 als Security Guard für BGP-Peering verwendet.
Textfeld „MD5-Kennwort (MD5 Password)“	Beim Aktivieren von MD5-Authentifizierung ist ein Kennwort erforderlich.



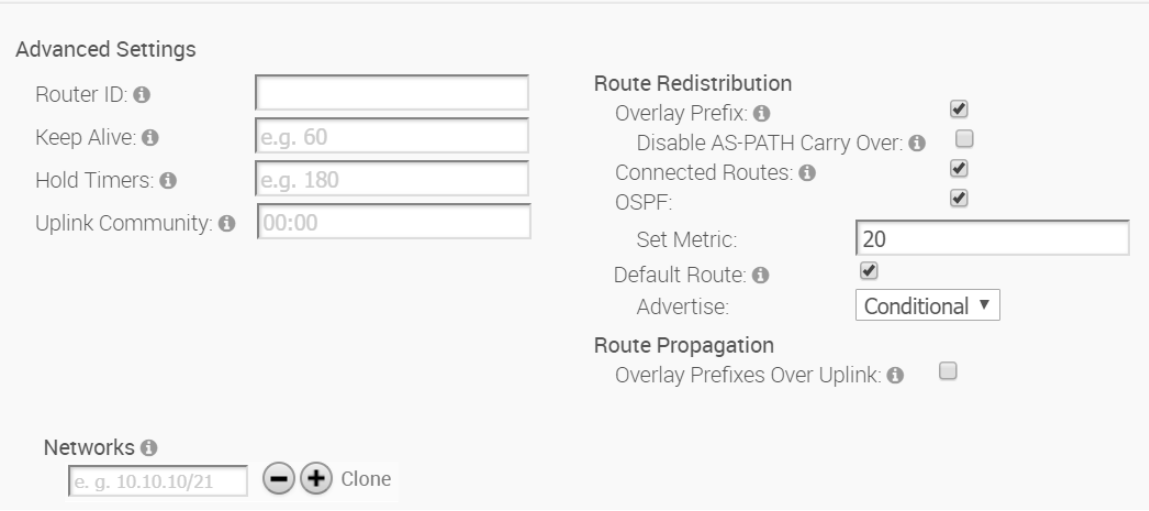
g Klicken Sie auf die Schaltfläche **Erweiterte Einstellungen (Advanced Settings)**.

Der Bereich **Erweiterte Einstellungen (Advanced Settings)** wird angezeigt.

h Im Bereich **Zusätzliche Einstellungen (Additional Settings)** können Sie die folgenden zusätzlichen BGP-Einstellungen eingeben, die in der nachstehenden Tabelle beschrieben werden. (Weitere Informationen hierzu finden Sie in nachstehender Abbildung.)

Felder unter **Zusätzliche Einstellungen (Additional Settings)**	**Beschreibung**
Router-ID (Router ID)	Wenn keine ID konfiguriert ist, wird diese automatisch zugewiesen.
Keep Alive	Die Häufigkeit (in Sekunden), mit der die Keepalive-Nachricht an den Peer gesendet wird. Der Standardwert beträgt 60 Sekunden. Der Bereich liegt zwischen 0 und 65535.
Hold-Timer (Hold Timers)	Intervall in Sekunden, in dem der Peer berücksichtigt wird, nachdem er keine Keepalive-Nachricht erhalten hat. Der Standardwert beträgt 180 Sekunden. Der Bereich liegt zwischen 0 und 65535.

Uplink-Community (Uplink Community)	Uplink bezieht sich auf einen Link, der mit dem Provider-Edge (PE) verbunden ist. Eingehende Routen (in Richtung des Edge), die dieser Community entsprechen, werden als Uplink-Routen behandelt. (Für die der Hub/Edge nicht als Besitzer angesehen wird.) Die Eingabe kann im ursprünglichen Zahlenformat oder im neuen AA:NN-Format erfolgen.
Overlay-Präfix (Overlay Prefix)	Verteilt die vom Overlay erlernten Präfixe neu.
AS-PATH-Übernahme deaktivieren (Disable AS-PATH Carry Over)	Diese Option sollte standardmäßig deaktiviert bleiben. In bestimmten Topologien beeinflusst die Deaktivierung der AS-Pfadübernahme den ausgehenden AS-PATH dahingehend, dass L3-Router einen Pfad in Richtung eines Edge oder Hubs bevorzugen. **Warnung: Wenn die AS-Pfadübernahme aktiviert ist, müssen Sie Ihr Netzwerk so konfigurieren, dass Routing-Schleifen vermieden werden.**
Verbundene Routen (Connected Routes)	Verteilt alle Subnetze der verbundenen Schnittstelle neu.
Kontrollkästchen „OSPF“	Aktiviert OSPF-Neuverteilung in BGP.
Standardroute (Default Route)	Verteilt die Standardroute nur dann neu, wenn der Edge Routen über Overlay oder Underlay erlernt.
Textfeld „Metrik festlegen (Set Metric)“	Optional können Sie OSPF aktivieren, wodurch OSPF-Routen in BGP eingefügt werden können. Die Standard-BGP-Metrik für die neu verteilten OSPF-Routen ist ein MED-Wert von 20.
Overlay-Präfixe über Uplink (Overlay Prefixes Over Uplink)	Uplink bezieht sich auf den Link/Nachbar, für den der Uplink mit dem Flag **Nachbar (Neighbor)** konfiguriert ist (in der Regel ist der Link mit dem PE-Router (Provider Edge) verbunden). Leitet Routen, die vom Overlay erlernt wurden, an den Uplink mit dem Flag **Nachbar (Neighbor)**.
Netzwerke (Networks)	Das Netzwerk, das von BGP im Format 10.10.10.10/21 angekündigt wird.



i Klicken Sie auf **OK**, um die Konfigurationen zu speichern.

Hinweis Wenn Sie das Kontrollkästchen **Standardroute (Default Route)** im Bereich **Zusätzliche Einstellungen (Additional Settings)** aktiviert haben, beachten Sie die folgenden vier Szenarien:

- Wenn die globale Option **Standardroute (Default Route)** mit der Option „Bedingt (Conditional)“ aktiviert ist und die Option **Standardroute (Default Route)** pro BGP-Nachbar nicht ausgewählt ist, verteilt BGP die Standardroute an seinen Nachbarn nur dann neu, wenn der Edge eine explizite Standardroute über Overlay oder Underlay erlernt.
- Wenn die globale Option **Standardroute (Default Route)** mit der Option „Bedingt (Conditional)“ aktiviert ist und die Option **Standardroute (Default Route)** pro BGP-Nachbar ausgewählt ist, überschreibt die Konfiguration „Pro Nachbar (Per Neighbor)“ die globale Konfiguration, obwohl „Standardroute immer bei BGP-Peer ankündigen (Advertise default route to BGP peer Always)“ ausgewählt ist.
- Wenn die globale Option **Standardroute (Default Route)** nicht aktiviert ist und die Option **Standardroute (Default Route)** pro BGP-Nachbar ausgewählt ist, kündigen Sie die Standardroute immer beim BGP-Peer an.
- Wenn die globale Option **Standardroute (Default Route)** nicht aktiviert ist und die Option **Standardroute (Default Route)** pro BGP-Nachbar nicht ausgewählt ist, kündigen Sie die Standardroute nicht beim BGP-Peer an bzw. verteilen Sie sie nicht neu.

Hinweis Alle oben aufgeführten Optionen sind auf Edge-Ebene verfügbar und können mit den Einstellungen unter „Edge-Überschreibung für BGP aktiviert (Edge override enabled for BGP)“ konfiguriert werden.

OSPF/BGP-Umverteilung

Die Routingprotokolle OSPF und BGP können unabhängig voneinander aktiviert werden, und das vorherige Modell, bei dem nur ein Routingprotokoll im System aktiviert werden darf, wurde mit dieser Version entfernt. Diese Version bietet auch die Möglichkeit der Umverteilung von OSPF in BGP oder BGP in OSPF (oder beides gleichzeitig) sowie andere mögliche Routenquellen wie über das Overlay gelernte Präfixe, verbundene Routen, statische Routen usw.

Darüber hinaus wird mit Version 3.2 das Umverteilungsverhalten entlang traditionellerer Wege standardisiert (ähnlich dem anderer Routinganbieter). Wenn z. B. mehr als eine Route für dasselbe Präfix verfügbar ist, wird nur die beste Route für dieses Präfix im System-RIB an das Zielprotokoll umverteilt, wenn die Konfiguration im Zielprotokoll die Umverteilung für diesen Routentyp zulässt.

Ziehen Sie beispielsweise die Umverteilung des Präfixes 192.168.1.0/24 in BGP in Erwägung. Angenommen, Routen zum Präfix 192.168.1.0/24 sind lokal verfügbar, von OSPF gelernt und separat als Overlay-Präfix gelernt. Gehen wir weiter davon aus, dass die OSPF-Route zwischen der OFC-Flow-Sortierung für das Präfix und den Routenmetriken und der Routenpräferenz höher rangiert als (besser ist als) die erlernte Overlay-Route für das gleiche Präfix. Anschließend wird die OSPF-Route in BGP umverteilt, wenn die OSPF-Umverteilung in BGP aktiviert wurde. Beachten Sie, dass das gelernte Overlay-Präfix nicht die beste Route für dieses Präfix im System-RIB ist und daher nicht in BGP umverteilt wird, selbst wenn die Umverteilung von Overlay-Präfixen in BGP aktiviert wurde.

Um in Fällen wie dem oben genannten die Umverteilung der besten Route für ein Präfix in ein bestimmtes Zielprotokoll zu erleichtern, kann der Benutzer die Umverteilung für den spezifischen Routentyp aktivieren, der die beste Route im System ist.

Wenn der Benutzer alternativ eine andere Routenquelle für das Präfix, das in das Zielprotokoll umverteilt werden soll, bevorzugt, kann er den relativen Vorrang der Route im System-RIB mit der Overlay-Flow-Steuerung, die von der Managementschnittstelle bereitgestellt wird, oder durch Variation der Routenmetrik steuern.

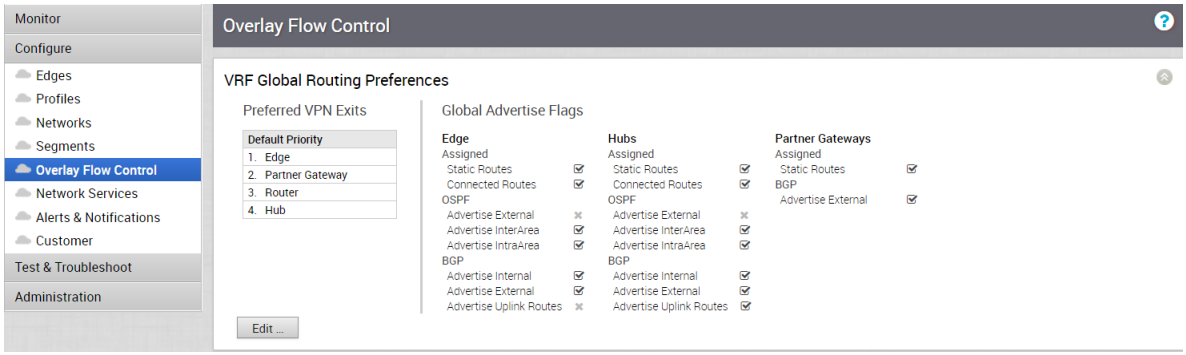
Weitere Informationen finden Sie unter Aktivieren von OSPF und BGP aktivieren.

Overlay-Flow-Steuerung

Im Bildschirm **Overlay-Flow-Steuerung (Overlay Flow Control)** wird eine Übersicht über alle Routen in Ihrem Netzwerk angezeigt.

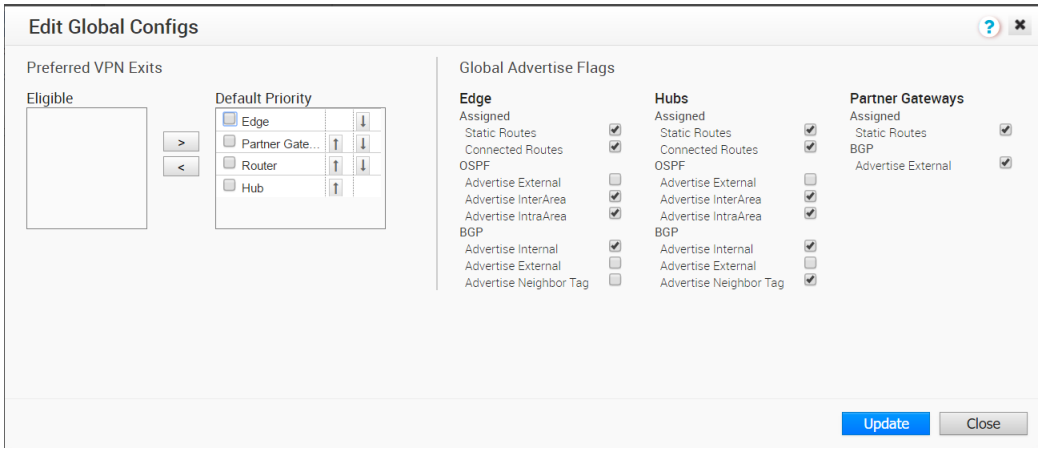
Einstellungen für globales Routing

In diesem Abschnitt werden die Einstellungen des globalen Routings beschrieben.



Einstellungen für Datenweiterleitung

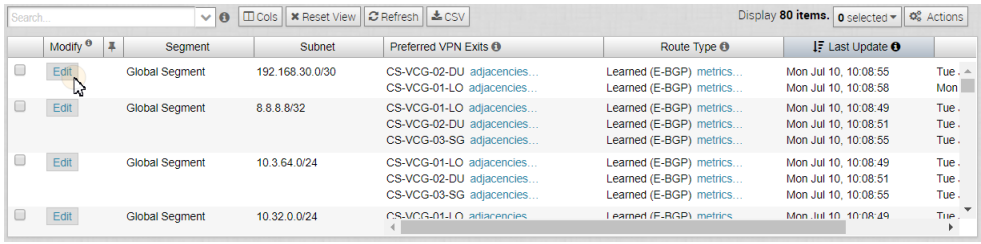
Im Bereich **Einstellungen für Datenweiterleitung (Data Forwarding Preferences)** legen Sie die Priorität der Ziele fest, für die der Datenverkehr geroutet werden soll. Klicken Sie zum Ändern der Priorität auf die Schaltfläche **Bearbeiten (Edit)** (siehe obige Abbildung), die sich unten im Bereich **Einstellungen für globales Routing (Global Routing Preferences)** befindet, um das Dialogfeld **Globale Konfigurationen bearbeiten (Edit Global Configs)** zu öffnen.



- „Intern ankündigen (Advertise Internal)“ verweist auf IBGP-Routen.
- „Extern ankündigen (Advertise external)“ verweist auf EBGP-Routen.
- „Uplink-Routen ankündigen (Advertise Uplink Routes)“ verweist auf Routen mit Uplink-Tag (U).

Tabelle „Overlay-Flow-Steuerung“ (Overlay Flow Control)

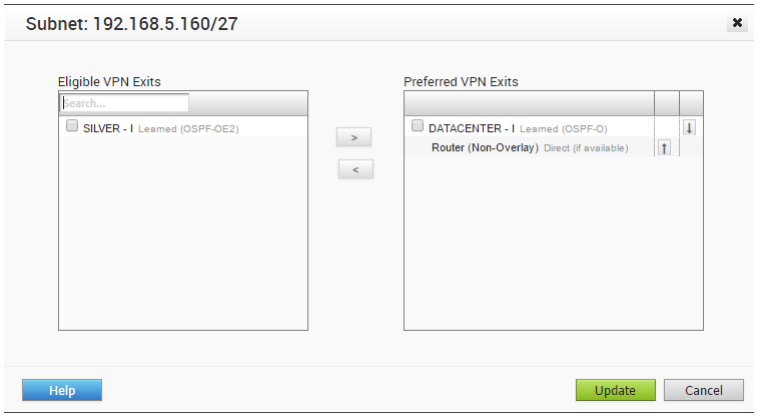
Alle Routen werden in der Tabelle **Overlay-Flow-Steuerung (Overlay Flow Control)** angezeigt. Dies umfasst Folgendes: Segment, Subnetz, Routentyp und Einstellungen.



Spaltenname	Beschreibung
Subnetz (Subnet)	Das Netzwerk, dem diese Route entspricht, zusammen mit einer Liste der Edges, die diese Route gelernt haben.
Routentyp (Route Type)	Verbunden: Ein Netzwerk, das direkt mit der Schnittstelle verbunden ist. Es gibt folgende Typen: OSPF-O, OSPF-OE2, BGP, Statisch und Verbunden.
Voreinstellungen (Preferences)	VMware SD-WAN (B2B) - VMware SD-WAN Route Direct: Direkte Schnittstellenroute, wenn eine private Verbindung vorhanden ist.

Bearbeiten von Routen

Sie können auch das Ziel Ihrer Einstellungen ändern. Klicken Sie in der Tabelle **Overlay-Flow-Steuerung (Overlay Flow Control)** auf die Schaltfläche **Bearbeiten (Edit)**. Wenn Sie die Zieleinstellung ändern, gilt die Änderung nur für die jeweilige Route bzw. das Subnetz.

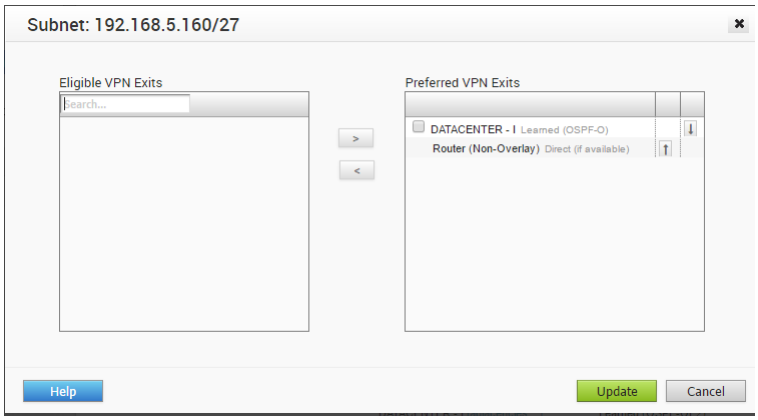


Nachbarschaften

Nachbarschaften zeigen Routen zwischen OSPF, BGP-Nachbarn und dem Edge an, wie in der folgenden Abbildung dargestellt. Klicken Sie auf den Link **Nachbarschaften (Adjacencies)**, um diese benachbarten Beziehungen anzuzeigen.

Erneutes Priorisieren von Routen

Sie können Routen erneut priorisieren, indem Sie im Bereich **Overlay-Flow-Steuerung (Overlay Flow Control)** auf die Schaltfläche **Bearbeiten (Edit)** klicken. Dies sind die letzten Ausgangspunkte, um das Zielsubnetz zu erreichen.



Schnellstartkonfiguration

20

In diesem Abschnitt werden die Schritte beschrieben, die für die erstmalige Edge-Konfiguration und -Aktivierung mithilfe von SD-WAN Orchestrator mindestens erforderlich sind. Sie sollten sich mit den Konzepten vertraut machen, die unter *Übersicht* erläutert werden, bevor Sie die in diesem Abschnitt beschriebenen Schritte ausprobieren.

Es gibt drei Schnellstart-Konfigurationsszenarien.

- SaaS
- Non VMware SD-WAN Site mit VPN
- VMware SD-WAN Site mit VPN

Weitere Informationen zu diesen Details finden Sie unter *Konfigurations-Workflow*.

In diesem Abschnitt wird jedes dieser Szenarien beschrieben. Der SD-WAN Orchestrator verfügt über Standardkonfigurationen für Netzwerke, Netzwerkdienste und Profile. Mithilfe dieser vordefinierten Konfigurationen können Sie eine SD-WAN Edge-Konfiguration erstellen und verfügen dann in wenigen Minuten über einen einsatzbereiten Edge.

In der folgenden Tabelle werden die Standardkonfigurationen beschrieben:

Konfiguration	Beschreibung
Netzwerkdienste (Network Services)	Konfiguration für Open DNS- und Google DNS-Dienste
Netzwerke (Networks)	Es werden zwei vorkonfigurierte Netzwerke bereitgestellt, jeweils mit einem Unternehmens- und einem Gastnetzwerk mit definiertem VLAN: ■ Internetnetzwerk: Konfiguration für ein Nicht-VPN Netzwerk mit sich überlappenden Adressen. ■ VPN-Netzwerk: Konfiguration für ein VPN-Netzwerk mit sich nicht überlappenden Adressen.
Profile (Profiles)	Es werden zwei vorkonfigurierte Profile bereitgestellt. Jedes davon verwendet ein vorkonfiguriertes Netzwerk und Netzwerkdienste und definiert LAN- und WLAN-Schnittstelleneinstellungen. Die vordefinierten Profile sind: ■ Schnellstart-Internetnetzwerk: Dieses Profil verwendet die Internetnetzwerkkonfiguration. ■ Schnellstart-VPN-Netzwerk: Dieses Profil verwendet die VPN-Netzwerkkonfiguration.

Dieses Kapitel enthält die folgenden Themen:

- Bereitstellen von Edges mit Non VMware SD-WAN Site-VPN-Profil
- Bereitstellen von Edges mit VMware SD-WAN Site-VPN-Profil
- Zero-Touch-Bereitstellung
- Aktivierung per Push

SaaS-Schnellstart

Ein Administrator kann einen Edge mit dem Standard-Internetnetzwerk, Netzwerkdiensten und Profilkonfigurationen bereitstellen und anschließend die Aktivierung auf dem Edge starten. In diesem Szenario muss nur ein Edge konfiguriert werden.

Führen Sie die folgenden Schritte aus:

1 Erstellen Sie einen Edge mithilfe des Internetprofils.

2 Senden Sie eine E-Mail zur Edge-Aktivierung.

In den folgenden Abschnitten werden diese Schritte genauer beschrieben.

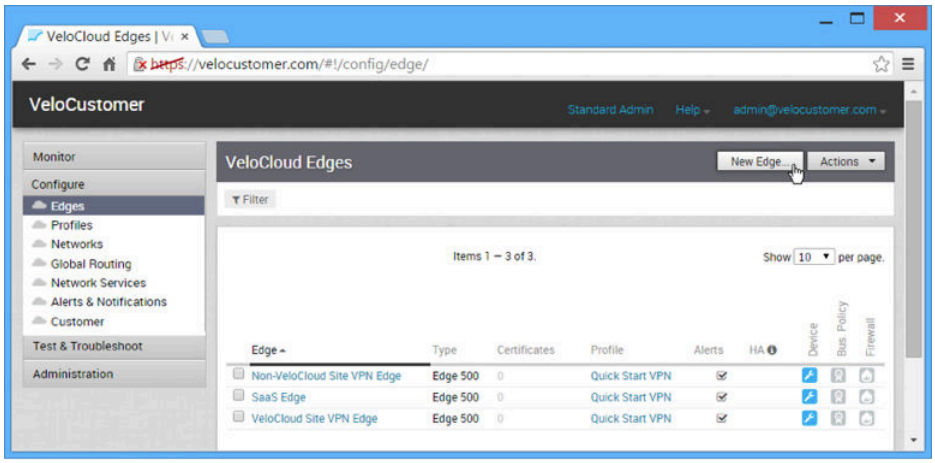
Erstellen eines Edge mithilfe des Internetprofils

In diesem Abschnitt wird beschrieben, wie Sie einen Edge mithilfe des Internetprofils erstellen.

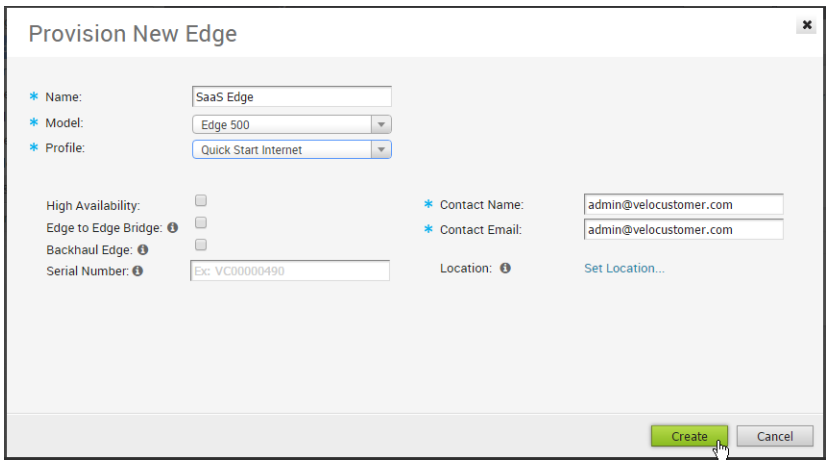
So erstellen Sie einen Edge mithilfe des Internetprofils:

1 Klicken Sie im Navigationsbereich auf der linken Seite der SD-WAN Orchestrator-Instanz auf **Konfigurieren -> Edges (Configure -> Edges)**.

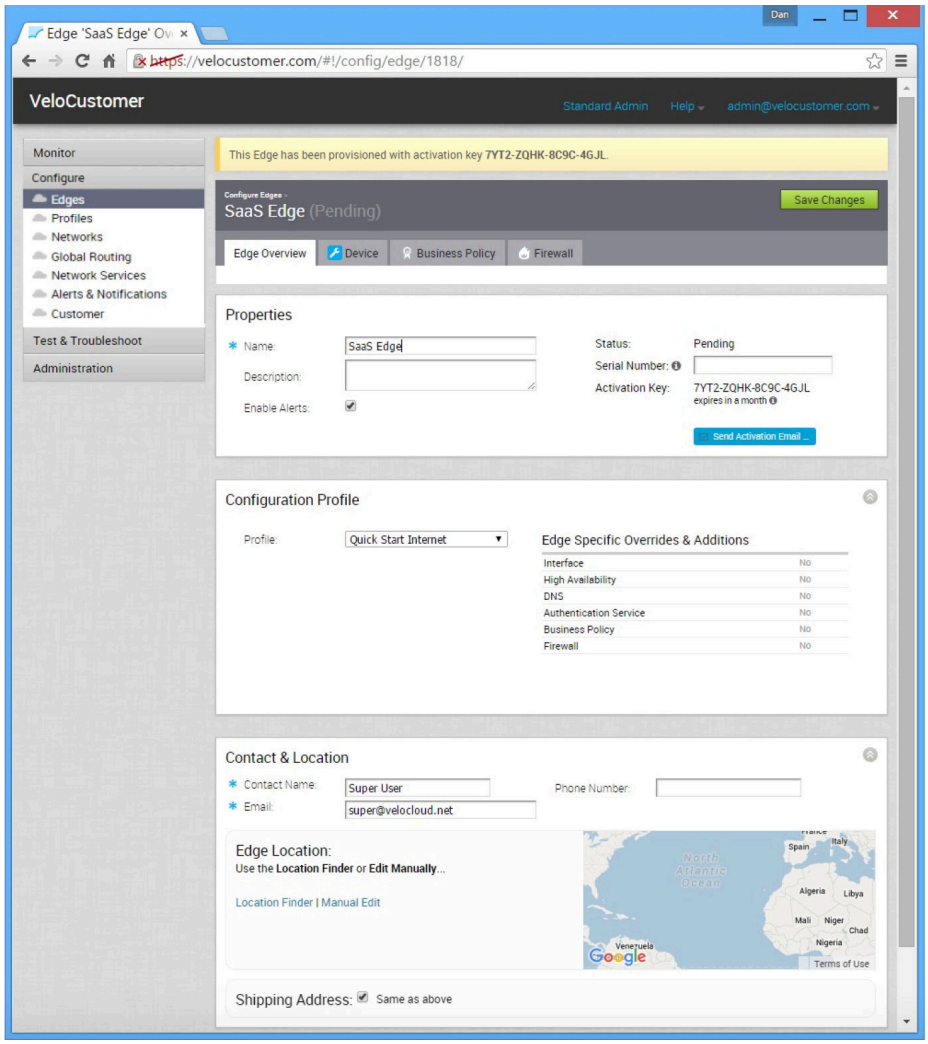
2 Klicken Sie auf der Seite „Edges“ oben rechts auf die Schaltfläche **Neuer Edge (New Edge)**.



3 Geben Sie im Dialogfeld „Neuen Edge bereitstellen (Provision New Edge)“ den Edge-Namen an, wählen Sie eine Edge-Modellnummer aus, wählen Sie die Option **Schnellstart-Internetprofil (Quick Start Internet Profile)** aus und geben Sie Ihren Namen und Ihre E-Mail-Adresse unter **Kontaktname (Contact Name)** und **Kontakt-E-Mail-Adresse (Contact Email)** ein.

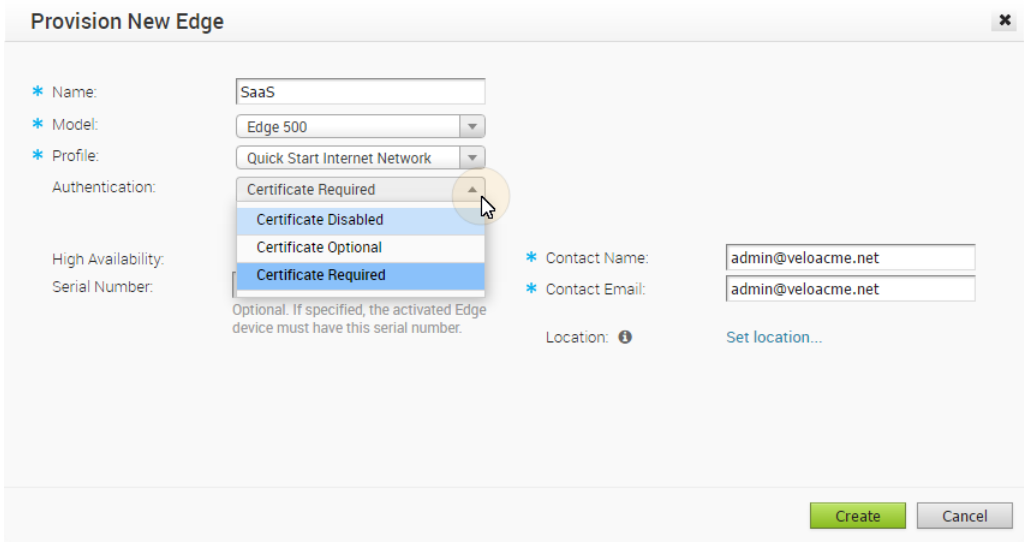


Die Beschreibung für den neu erstellten Edge wird angezeigt.

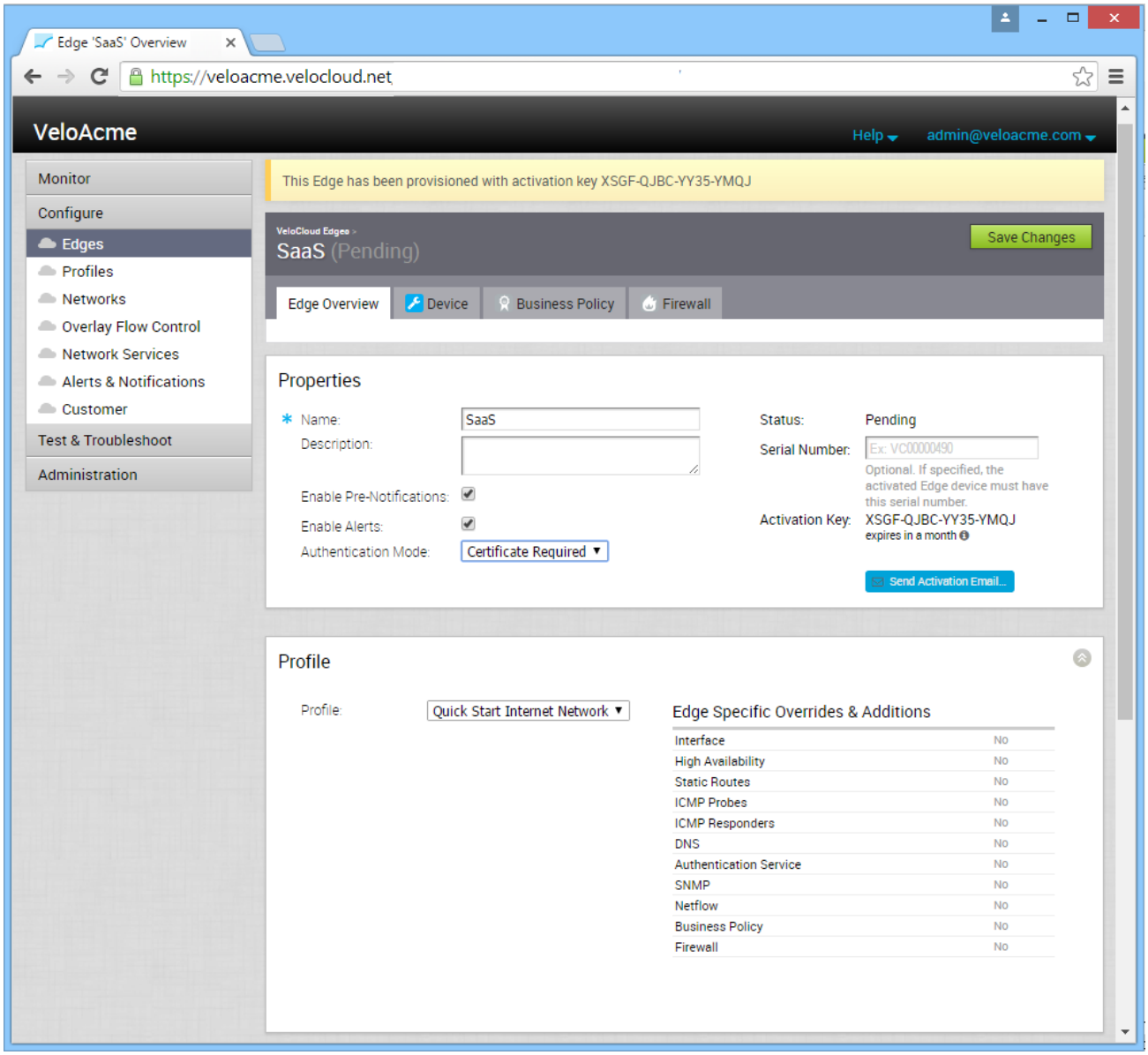


Mit der vorkonfigurierten Konfiguration für Netzwerke, Netzwerkdienste und Profile sowie der Standardkonfiguration für einen Edge ist Ihre neu erstellte Edge-Konfiguration vollständig. Sie sind jetzt in der Lage, Ihr Edge-Gerät zu aktivieren und die Konfiguration auf das Edge-Gerät anzuwenden. Die Edge-Aktivierung ist für die drei Workflows identisch. Führen Sie als Nächstes die unter Konfigurieren der Edge-Aktivierung beschriebenen Schritte aus.

Wenn PKI aktiviert ist, können Sie drei Zertifikatsoptionen auswählen (**Zertifikat erforderlich (Certificate Required)**, **Zertifikat optional (Certificate Optional)** oder **Zertifikat deaktiviert (Certificate Disabled)**). Wenn PKI aktiviert ist und Sie das Zertifikat auf **Zertifikat erforderlich (Certificate Required)** festlegen, stellen Sie den Edge bereit und der vorinstallierte Schlüssel ist nicht verfügbar.



Der neu erstellte Edge wird angezeigt.



Bereitstellen von Edges mit Non VMware SD-WAN Site-VPN-Profil

Ein Administrator kann einen Edge mit Standard-VPN-Netzwerk, Netzwerkdiensten und Profilkonfigurationen bereitstellen und anschließend die Aktivierung auf dem Edge starten. In diesem Szenario muss ein neues Profil konfiguriert werden, und ein Edge muss bereitgestellt werden.

Führen Sie die folgenden Schritte aus:

1 Erstellen Sie ein Non VMware SD-WAN Site-Profil.

2 Konfigurieren Sie die Non VMware SD-WAN Site über VPN.

3 Erstellen Sie einen Edge mithilfe des Non VMware SD-WAN Site-Profils.

4 Senden Sie eine E-Mail zur Edge-Aktivierung.

In den folgenden Abschnitten werden diese Schritte genauer beschrieben.

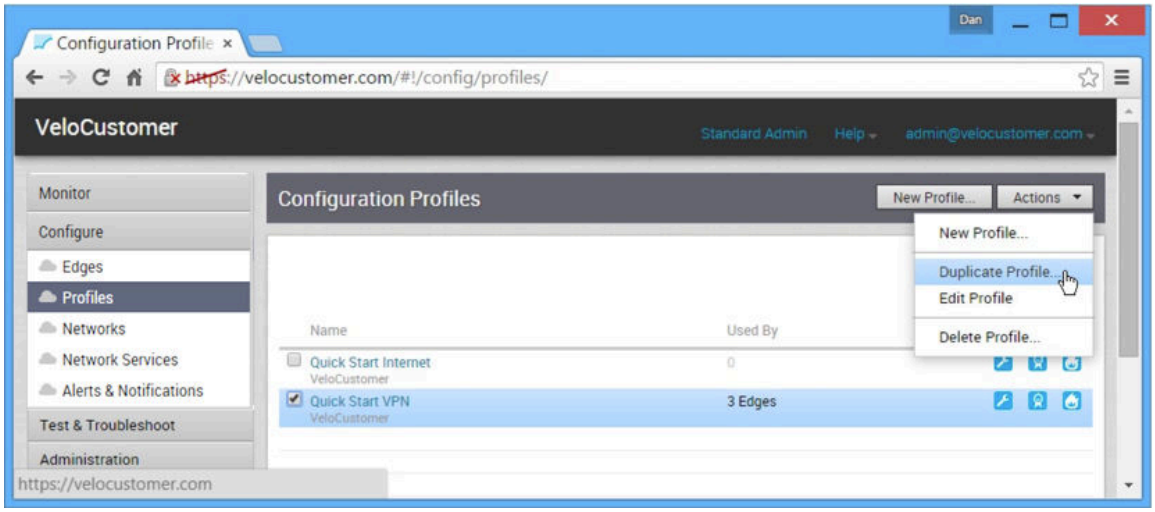
Erstellen eines Profils

In diesem Abschnitt wird beschrieben, wie Sie ein Profil erstellen.

So erstellen Sie ein Profil:

1 Klicken Sie im Navigationsbereich auf der linken Seite der SD-WAN Orchestrator-Instanz auf **Konfigurieren -> Profile (Configure -> Profiles)**.

2 Wählen Sie auf der Seite „Konfigurationsprofile (Configuration Profiles)“ die Option **Schnellstart-VPN-Profil (Quick Start VPN Profile)** aus und klicken Sie oben rechts auf **Aktionen -> Profil duplizieren (Actions -> Duplicate Profile)**.



Konfigurieren über VPN

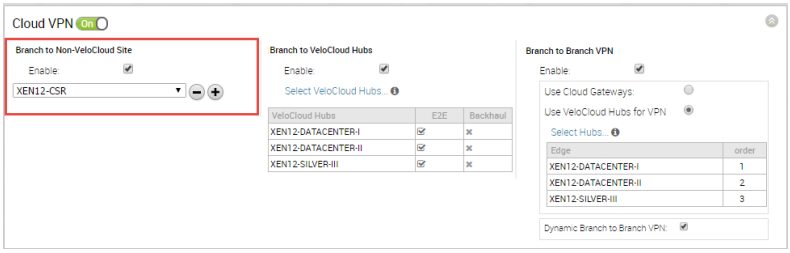
In diesem Abschnitt wird die Konfiguration über VPN beschrieben.

So konfigurieren Sie über VNP:

1 Wählen Sie die Registerkarte **Gerät (Device)** des Profils aus.

2 Aktivieren Sie **Cloud-VPN (Cloud VPN)**.

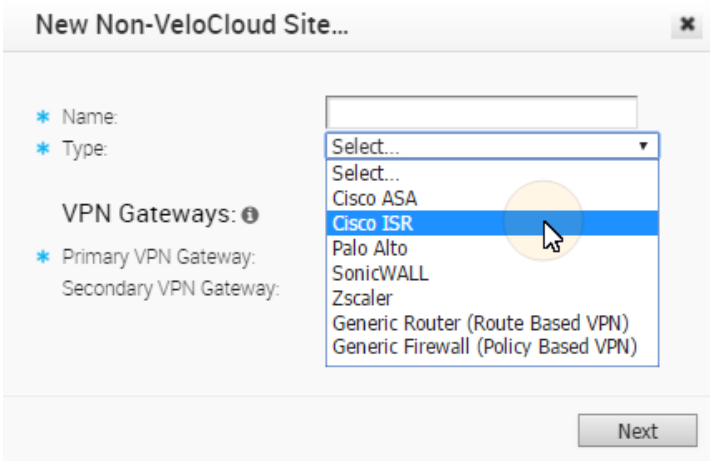
3 Aktivieren Sie den Edge für Non VMware SD-WAN Site und wählen Sie dann **Neu (New)** Non VMware SD-WAN Site aus.



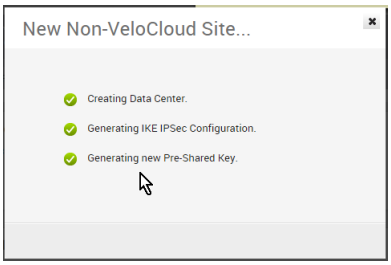
4 Klicken Sie im Navigationsbereich auf der linken Seite der SD-WAN Orchestrator-Instanz auf **Konfigurieren -> Profile (Configure -> Profiles)**.

5 Wählen Sie auf der Seite „Profile (Profiles)“ die Option **Schnellstart-VPN-Profil (Quick Start VPN Profile)** aus und klicken Sie dann oben rechts auf **Aktionen -> Profil duplizieren (Actions -> Duplicate Profile)**.

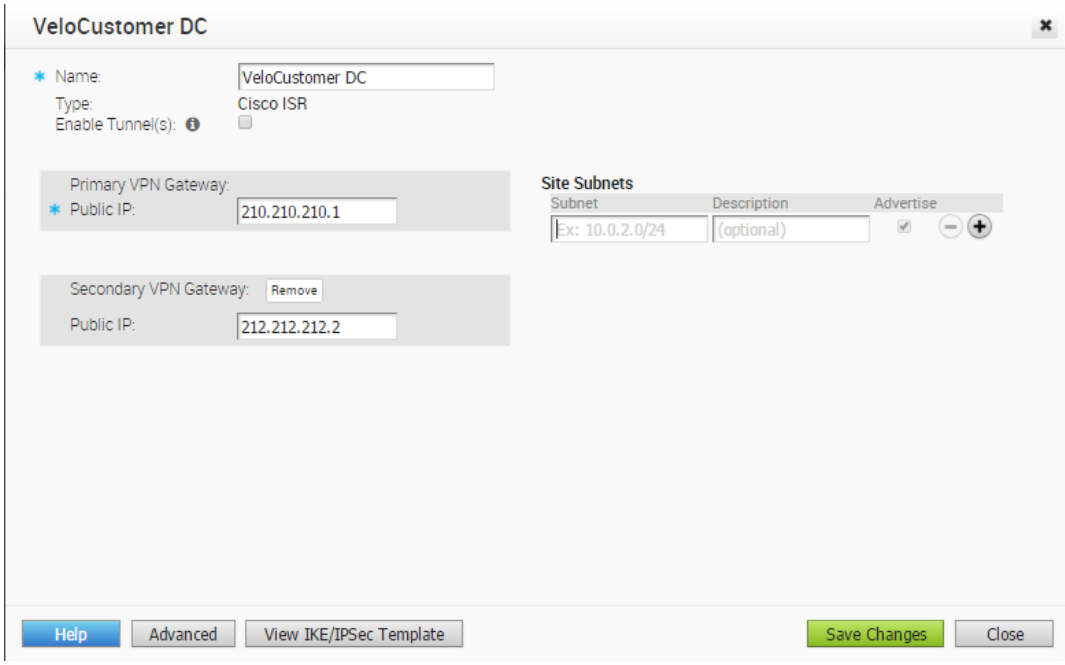
6 Wählen Sie einen **Typ (Type)** für die Non VMware SD-WAN Site aus. Im folgenden Beispiel wird ein Cisco ISR ausgewählt. Geben Sie zusätzliche Parameter ein, die für die von Ihnen ausgewählte Non VMware SD-WAN Site erforderlich sind, und klicken Sie auf **Weiter (Next)**.



Es wird ein Status für die Erstellung der neuen Non VMware SD-WAN Site angezeigt.



Ein abschließendes Dialogfeld für die Fertigstellung der Konfiguration der Non VMware SD-WAN Site wird angezeigt.



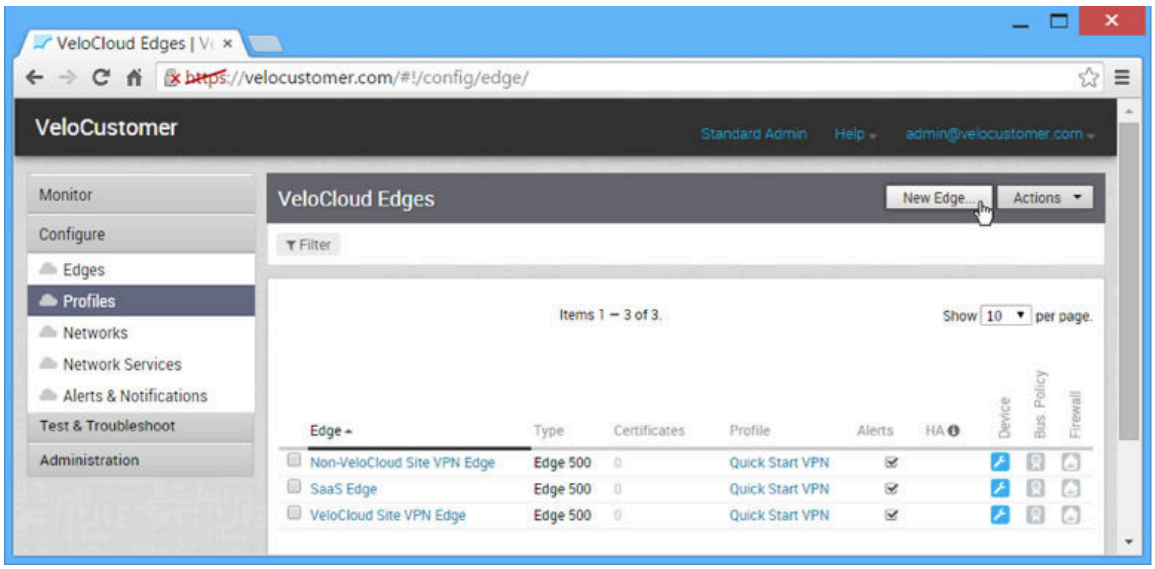
Erstellen eines Edge mit dem VPN-Profil

In diesem Abschnitt wird beschrieben, wie Sie einen Edge mithilfe des VPN-Profils erstellen.

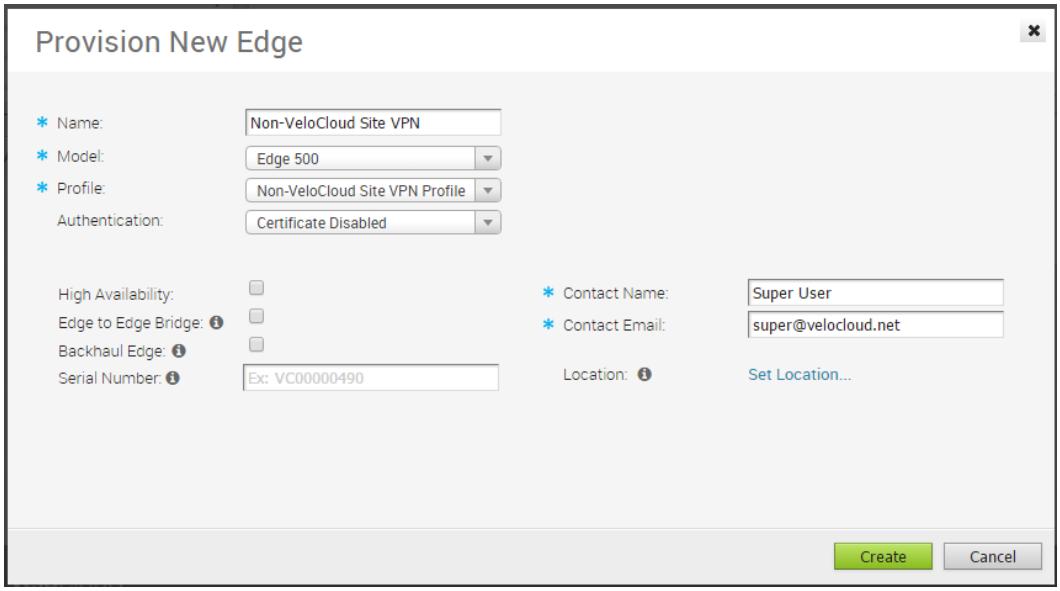
So erstellen Sie einen Edge mithilfe des VPN-Profils:

1 Klicken Sie im Navigationsbereich auf der linken Seite der SD-WAN Orchestrator-Instanz auf **Konfigurieren (Configure) -> Profile (Profiles)**.

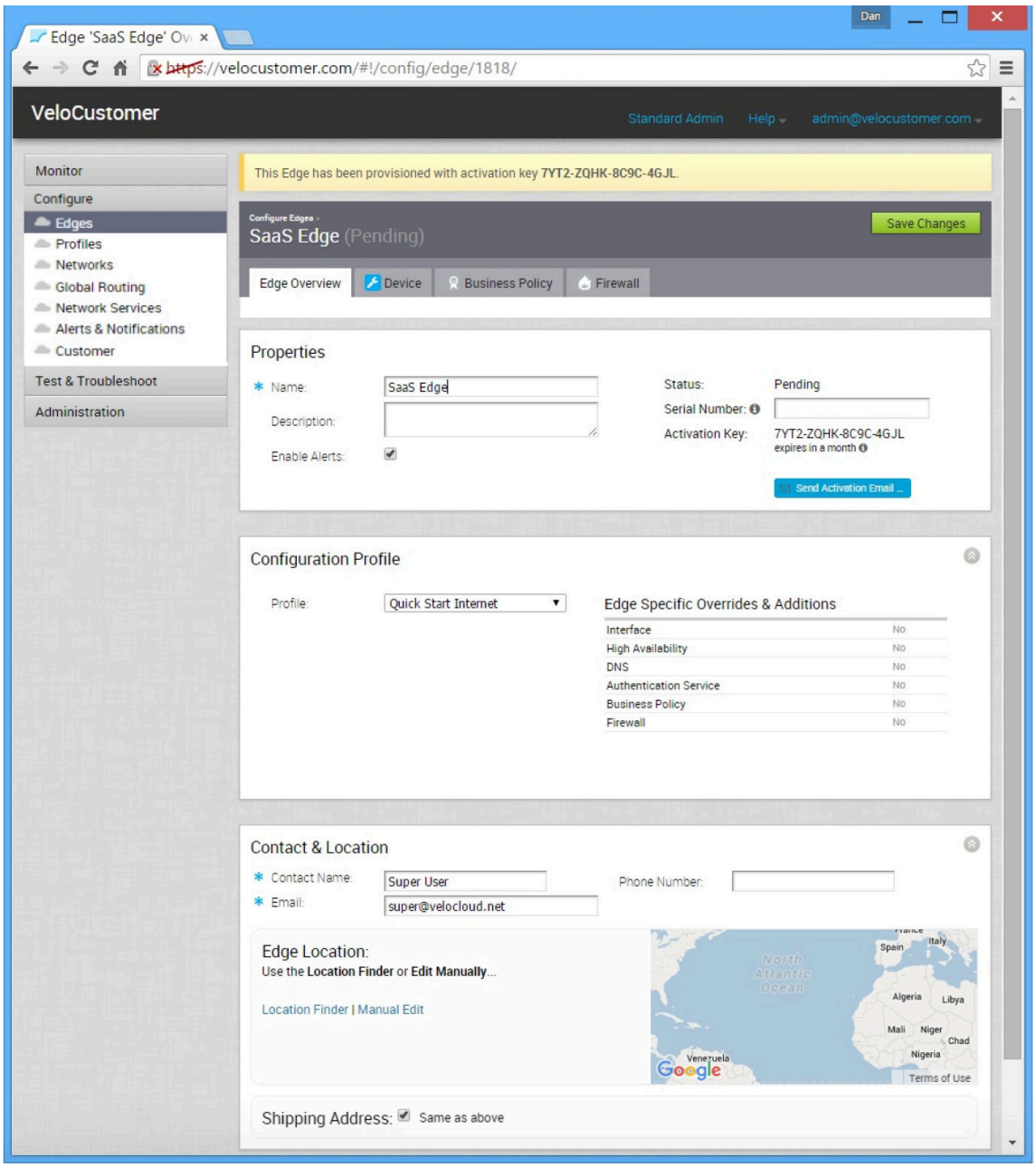
2 Klicken Sie oben rechts auf die Schaltfläche **Neuer Edge (New Edge)**.



3 Geben Sie im Dialogfeld „Neuen Edge bereitstellen (Provision New Edge)“ Ihren Edge-Namen an, wählen Sie eine Edge-Modellnummer aus, wählen Sie die Option **Schnellstart-VPN-Profil (Quick Start VPN Profile)** aus und geben Sie Ihren Namen und Ihre E-Mail-Adresse unter **Kontaktname (Contact Name)** und **Kontakt-E-Mail-Adresse (Contact Email)** ein.



Die Beschreibung für den neu erstellten Edge wird angezeigt.



Mit der vorkonfigurierten Konfiguration für Netzwerke, Netzwerkdienste und Profile sowie der Standardkonfiguration für einen Edge ist Ihre neu erstellte Edge-Konfiguration vollständig. Der einzige verbleibende Schritt stellt die Aktivierung des Edge dar. Die Edge-Aktivierung ist für die drei Szenarios identisch. Führen Sie als Nächstes die unter Konfigurieren der Edge-Aktivierung beschriebenen Schritte aus.

Bereitstellen von Edges mit VMware SD-WAN Site-VPN-Profil

Ein Administrator kann einen Edge mit Standard-VPN-Netzwerk, Netzwerkdiensten und Profilkonfigurationen bereitstellen und anschließend die Aktivierung auf dem Edge starten. In

diesem Szenario muss ein neues Profil konfiguriert werden, und ein Edge muss bereitgestellt werden.

Führen Sie die folgenden Schritte aus:

1 Erstellen Sie ein VMware SD-WAN Site-Profil.

2 Konfigurieren Sie das VMware SD-WAN Site-VPN-Profil.

3 Stellen Sie einen Edge mithilfe des VMware SD-WAN Site-VPN-Profils bereit.

4 Senden Sie eine E-Mail zur Edge-Aktivierung.

In den folgenden Abschnitten werden diese Schritte genauer beschrieben.

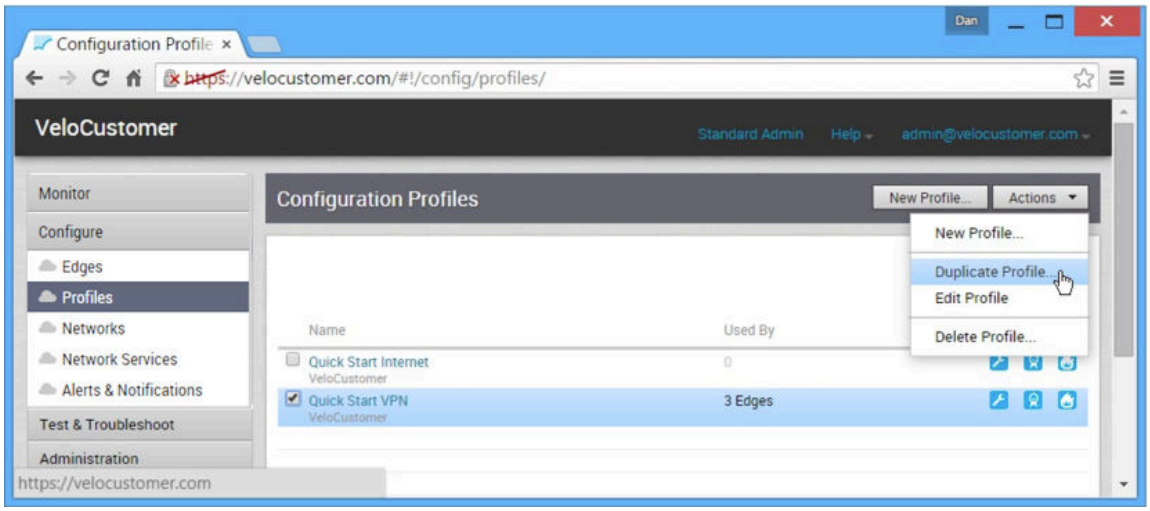
Erstellen eines Profils

In diesem Abschnitt wird beschrieben, wie Sie ein Profil erstellen.

So erstellen Sie ein Profil:

1 Klicken Sie im Navigationsfenster auf der linken Seite der SD-WAN Orchestrator-Instanz auf **Konfigurieren -> Profile (Configure -> Profiles)**, um ein VMware SD-WAN Site-Profil zu erstellen.

2 Um ein doppeltes Profil zu erstellen, wählen Sie auf der Seite „Konfigurationsprofile (Configuration Profiles)“ die Option **Schnellstart-VPN-Profil (Quick Start VPN Profile)** aus und klicken Sie oben rechts auf **Aktionen -> Profil duplizieren (Actions -> Duplicate Profile)**.



Konfigurieren des VPN-Profils

In diesem Abschnitt wird beschrieben, wie Sie das VPN-Profil konfigurieren.

Das VMware SD-WAN Site-VPN kann für zwei Typen von VMware SD-WAN Site-VPNs konfiguriert werden:

- Zweigstelle-zu-Hubs

- Zweigstelle-zu-Zweigstelle-VPN

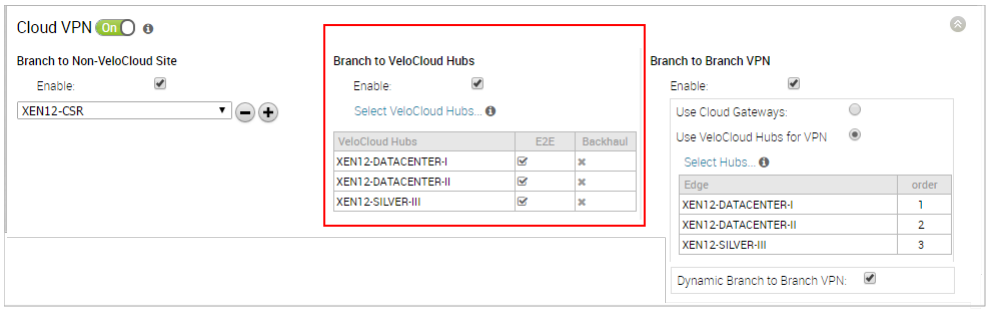
Hinweis Die Funktion „Cloud-VPN (Cloud VPN)“ auf der Registerkarte **Gerät (Device)** muss auf **Ein (On)** gesetzt sein, um die Konfigurationsoptionen für die beiden VPN-Typen anzuzeigen.

Konfigurieren von Zweigstelle-zu-Hubs

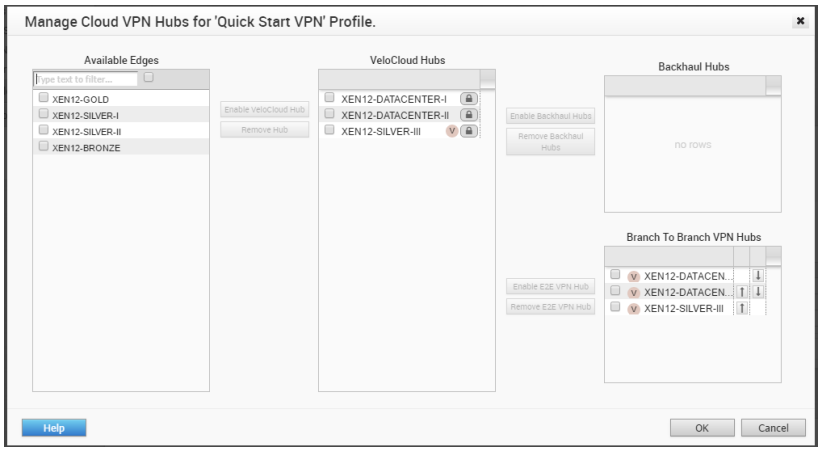
So konfigurieren Sie das VPN-Profil für Zweigstelle-zu-Hubs:

1 Aktivieren Sie unter **Zweigstelle-zu-Hubs (Branch to Hubs)** das Kontrollkästchen **Aktivieren (Enable)**.

2 Klicken Sie auf die Schaltfläche **Edges auswählen (Select Edges)**.



Das folgende Dialogfeld wird angezeigt, in dem Sie zur Auswahl des SD-WAN Hubs aufgefordert werden, der für VPN-Tunnel zwischen den Edges mit diesem Profil und dem SD-WAN Edges verwendet werden kann, der als SD-WAN Hubs deklariert wurde.

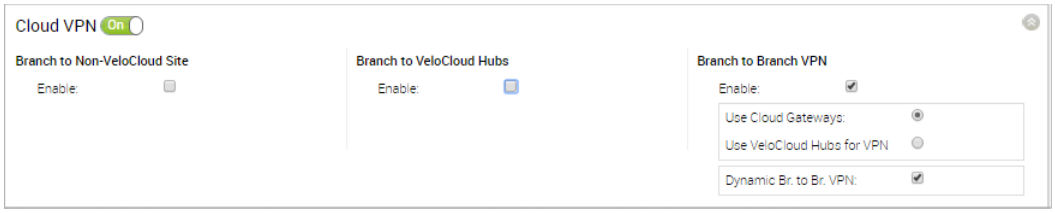


3 Nehmen Sie eine Auswahl vor und klicken Sie dann auf **OK**.

Konfigurieren eines Zweigstelle-zu-Zweigstelle-VPNs

So konfigurieren Sie das VPN-Profil für Zweigstelle-zu-Zweigstelle-VPN:

1 Wie in der folgenden Abbildung gezeigt (ganz rechts), konfigurieren Sie das Zweigstelle-zu-Zweigstelle-VPN, indem Sie das Kontrollkästchen **Aktivieren (Enable)** aktivieren.



2 Wählen Sie die Optionen **Cloud-Gateways verwenden (Use Cloud Gateways)** und SD-WAN Hub **Dynamisches Zweigstelle-zu-Zweigstelle-VPN (Dynamic Branch to Branch VPN)** aus.

3 Klicken Sie auf **OK**.

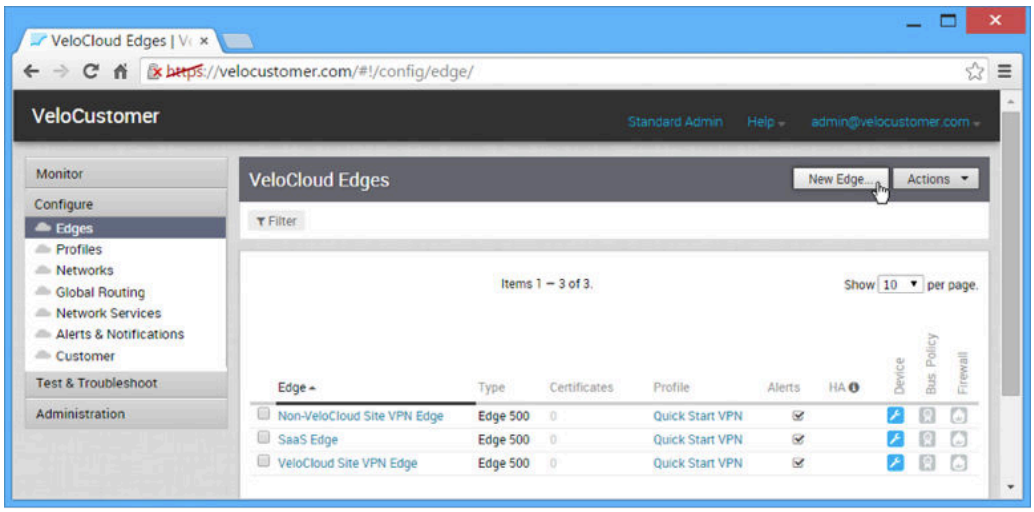
Erstellen eines Edge mithilfe des VPN-Profils

In diesem Abschnitt wird beschrieben, wie Sie einen Edge mithilfe des VPN-Profils erstellen.

So erstellen Sie einen Edge mithilfe des VPN-Profils:

1 Klicken Sie im Navigationsbereich auf der linken Seite der SD-WAN Orchestrator-Instanz auf **Edges**.

2 Klicken Sie auf der Seite „Edges“ oben rechts auf die Schaltfläche **Neuer Edge (New Edge)**.



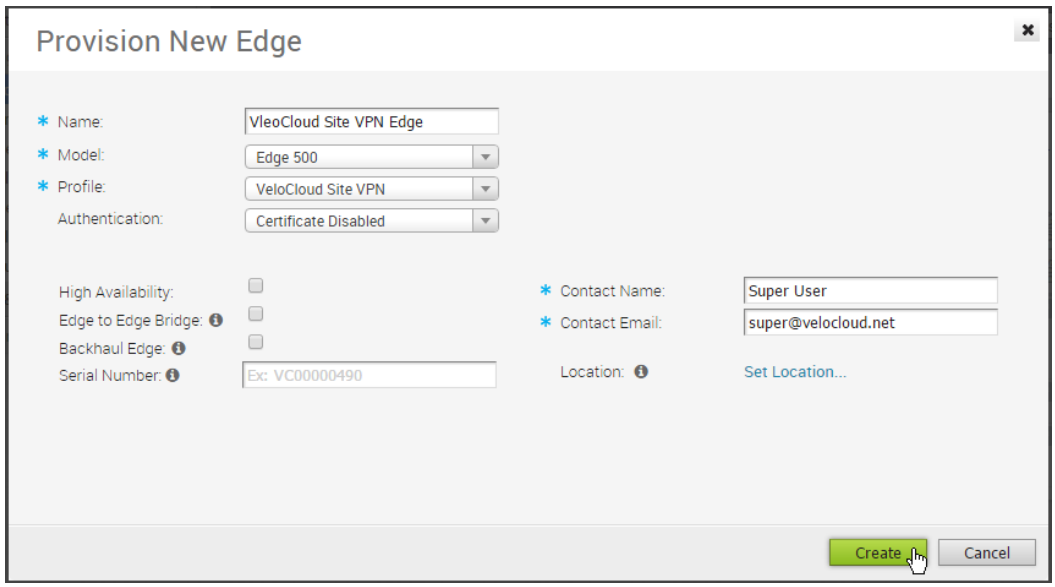
3 Führen Sie im Dialogfeld **Neuen Edge bereitstellen (Provision New Edge)** die folgenden Schritte aus:

a Geben Sie einen Namen für den **Edge** ein.

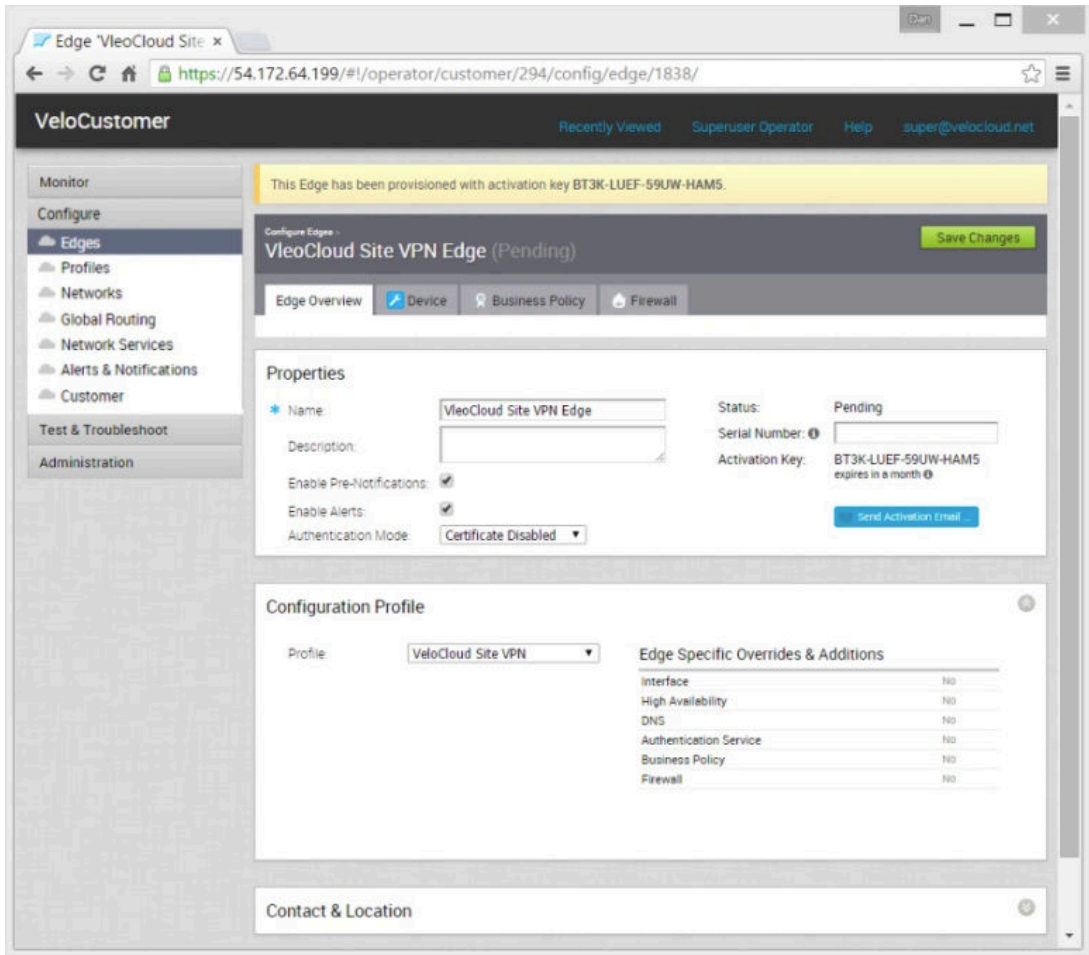
b Wählen Sie aus dem Dropdown-Menü eine Nummer für das **Edge-Modell (Edge Model)** aus.

c Wählen Sie das **Schnellstartprofil (Quick Start Profile)** aus dem Dropdown-Menü aus.

d Füllen Sie die Felder **Kontaktname (Contact Name)** und **Kontakt-E-Mail-Adresse (Contact Email)** aus.



Die Beschreibung für den neu erstellten Edge wird angezeigt.



Mit der vorkonfigurierten Konfiguration für Netzwerke, Netzwerkdienste und Profile sowie der Standardkonfiguration für einen Edge ist Ihre neu erstellte Edge-Konfiguration vollständig. Der einzige verbleibende Schritt stellt die Aktivierung des Edge dar. Die Edge-Aktivierung ist für die drei Szenarios identisch. Führen Sie als Nächstes die unter Konfigurieren der Edge-Aktivierung beschriebenen Schritte aus.

Zero-Touch-Bereitstellung

Die VMware SD-WAN-Lösung unterstützt zwei Methoden der SD-WAN Edge-Zero-Touch-Bereitstellung und -Aktivierung: Aktivierung per Pull und Aktivierung per Push

Aktivität	Aktivierung per Pull (Aktivierung durch Office-Administrator)	Aktivierung per Push (Zentrale NOC-Aktivierung)
Kein IT-Besuch erforderlich	✓	✓
Kein Vorab-Staging erforderlich	✓	✓
Kein Sicherheitsrisiko bei Verlust von Box	✓	✓
Kein Site-by-Site-Verbindungsprofil erforderlich	✓	✓
Keine Geräteverfolgung erforderlich	✓	
Erfordert E-Mail an Office-Administrator	✓	
Erfordert Kenntnisse über Gerät für Site	✓	✓

Aktivierung per Pull

Bei der Pull-Aktivierungsmethode wird der SD-WAN Edge mit einer werkseitigen Standardkonfiguration an den Kundenstandort geliefert. Vor der Aktivierung enthält der SD-WAN Edge keine Konfiguration oder Anmeldedaten, um eine Verbindung mit dem Unternehmensnetzwerk herzustellen.

Der Aktivierungsvorgang für den Edge per Pull besteht aus den folgenden Schritten:

1 Senden Sie eine Aktivierungsmail.

   Der Administrator startet den Aktivierungsvorgang, indem er eine E-Mail mit dem Aktivierungsverfahren an die Person sendet, die den Edge installiert. In der Regel ist dies ein Site-Kontakt.

2 Aktivieren Sie das Edge-Gerät.

   Die Person, die die Anweisungen in der E-Mail mit dem Aktivierungsverfahren ausführt, aktiviert das Edge-Gerät.

Führen Sie die folgenden Anweisungen für den Edge-Aktivierungsvorgang per Pull aus.

Senden einer Aktivierungs-E-Mail

Der Vorgang zur Aktivierung des Edge beginnt mit der Einleitung eines Aktivierungsverfahrens mithilfe einer E-Mail, die vom IT-Administrator an den Site-Kontakt gesendet wird.

So senden Sie die E-Mail für das Aktivierungsverfahren:

1 Navigieren Sie über den Orchestrator zu **Konfigurieren (Configure) > Edges**.

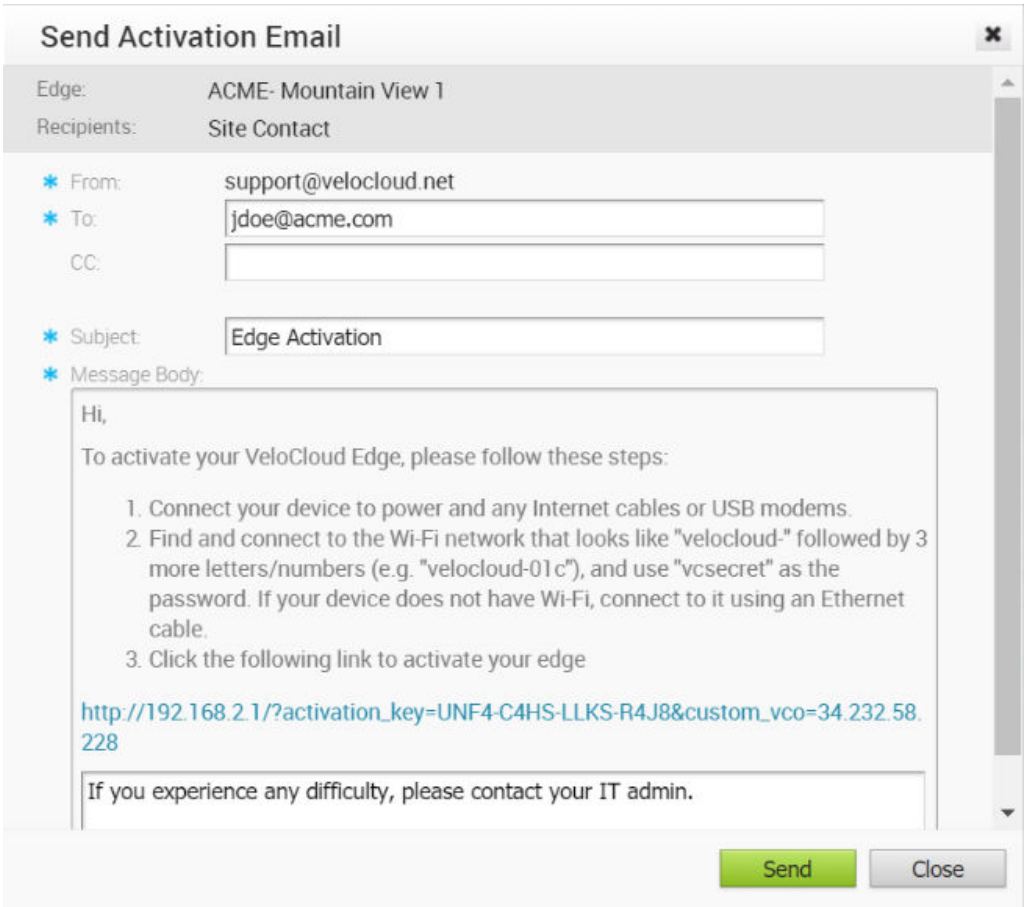
2 Wählen Sie den Edge aus, den Sie aktivieren möchten. Das Fenster mit der Registerkarte **Edge-Übersicht (Edge Overview)** wird angezeigt.

3 Geben Sie als optionalen Schritt im Bereich **Eigenschaften (Properties)** die Seriennummer des Edge, der aktiviert wird, im Textfeld **Seriennummer (Serial Number)** ein. Bei den Seriennummern wird die Groß-/Kleinschreibung beachtet. Geben Sie daher „VC“ unbedingt in Großbuchstaben ein.

Hinweis Dieser Schritt ist optional. Wird die Seriennummer angegeben, muss sie jedoch mit dem aktivierten Edge übereinstimmen.

4 Klicken Sie auf die Schaltfläche **Aktivierungs-E-Mail senden**, um die Aktivierungs-E-Mail an den Site-Kontakt zu senden.

5 Das Popup-Fenster **Aktivierungs-E-Mail senden (Send Activation Email)** wird angezeigt. Hier werden die Schritte beschrieben, die der Site-Kontakt ausführen muss, um das Edge-Gerät zu aktivieren.



Hinweis Wenn in Version 3.4 ein Edge 510 LTE-Gerät konfiguriert wurde, enthält die Aktivierungs-E-Mail Mobilfunkeinstellungen (z. B. SIM-PIN, Netzwerk, APN, Benutzername).

6 Klicken Sie auf die Schaltfläche **Senden (Send)**, um die Aktivierungs-E-Mail an den Site-Kontakt zu senden.

Hinweis Wenn Sie das Edge 510 LTE-Gerät konfigurieren, können Sie zu Fehlerbehebungszwecken den Diagnosetest „LTE-Modeminformationen (LTE Modem Information)“ ausführen. Während des Diagnosetests **LTE-Modeminformationen (LTE Modem Information)** werden Diagnoseinformationen abgerufen, wie z. B. Signalstärke, Verbindungsinformationen usw. Informationen zum Ausführen eines Diagnosetests finden Sie im Abschnitt Remote-Diagnose.

Aktivieren eines Edge-Geräts

Der Site-Kontakt führt die in der E-Mail zum Edge-Aktivierungsverfahren beschriebenen Schritte aus.

Im Allgemeinen führt der Site-Kontakt die folgenden Schritte aus:

1 Schließen Sie Ihr Edge-Gerät an das Stromnetz an und stecken Sie alle Internetkabel oder USB-Modems ein.

2 Suchen und verbinden Sie sich mit dem WLAN-Netzwerk, das wie `velocloud–` aussieht, gefolgt von drei weiteren Buchstaben/Zahlen (zum Beispiel `velocloud–01c`), mit dem Kennwort `vcsecret`.

3 Klicken Sie auf den Hyperlink in der E-Mail, um den Edge zu aktivieren.

Hinweis Weitere Informationen finden Sie in der im Lieferumfang enthaltenen WLAN-SSID. Das Standard-WLAN ist `vc–wifi`.

Die E-Mail zur Edge-Aktivierung enthält möglicherweise spezifische Anweisungen zum Anschluss von WAN-Kabeln und USB-Modems, zum Anschluss von Geräten an die LAN-Verbindungen und zum Anschluss zusätzlicher Netzwerkgeräte an den Edge. Sie kann auch Anweisungen für die Verwendung einer oder mehreren WLAN-Verbindungen enthalten.

Während der Aktivierung des Edge wird der Bildschirm „Aktivierungsstatus (activation status)“ angezeigt.

Der Edge lädt die Konfiguration und Software aus dem SD-WAN Orchestrator herunter. Der Edge wird erfolgreich aktiviert und ist dann einsatzbereit. Sobald ein Edge aktiviert wurde, kann er für das Routing des Netzwerkdatenverkehrs verwendet werden. Darüber hinaus werden erweiterte Funktionen wie Überwachung, Testen und Fehlerbehebung aktiviert.

Aktivierung per Push

Für die Push-Aktivierungsmethode wird der SD-WAN Edge aktiviert, ohne dass ein Office-Administrator auf einen Aktivierungslink klicken muss.

Einige Szenarien, bei denen eine Aktivierung per Push erforderlich ist:

- Wenn ein Dienstanbieter die physische Installation von Geräten an einem Standort auslagert – in den meisten Fällen nur, um Kabel und die Stromversorgung anzuschließen. Die Person, die das Gerät installiert, ist möglicherweise weder ein Mitarbeiter des Endkunden noch des Dienstanbieters.
- Wenn die Person am Remote-Standort ein Laptop/Tablet/Smartphone nicht mit dem SD-WAN Edge verbinden kann und daher keine E-Mail-Adresse verwenden oder nicht auf einen Aktivierungscode bzw. eine URL klicken kann.

Konfigurieren von Warnungen

21

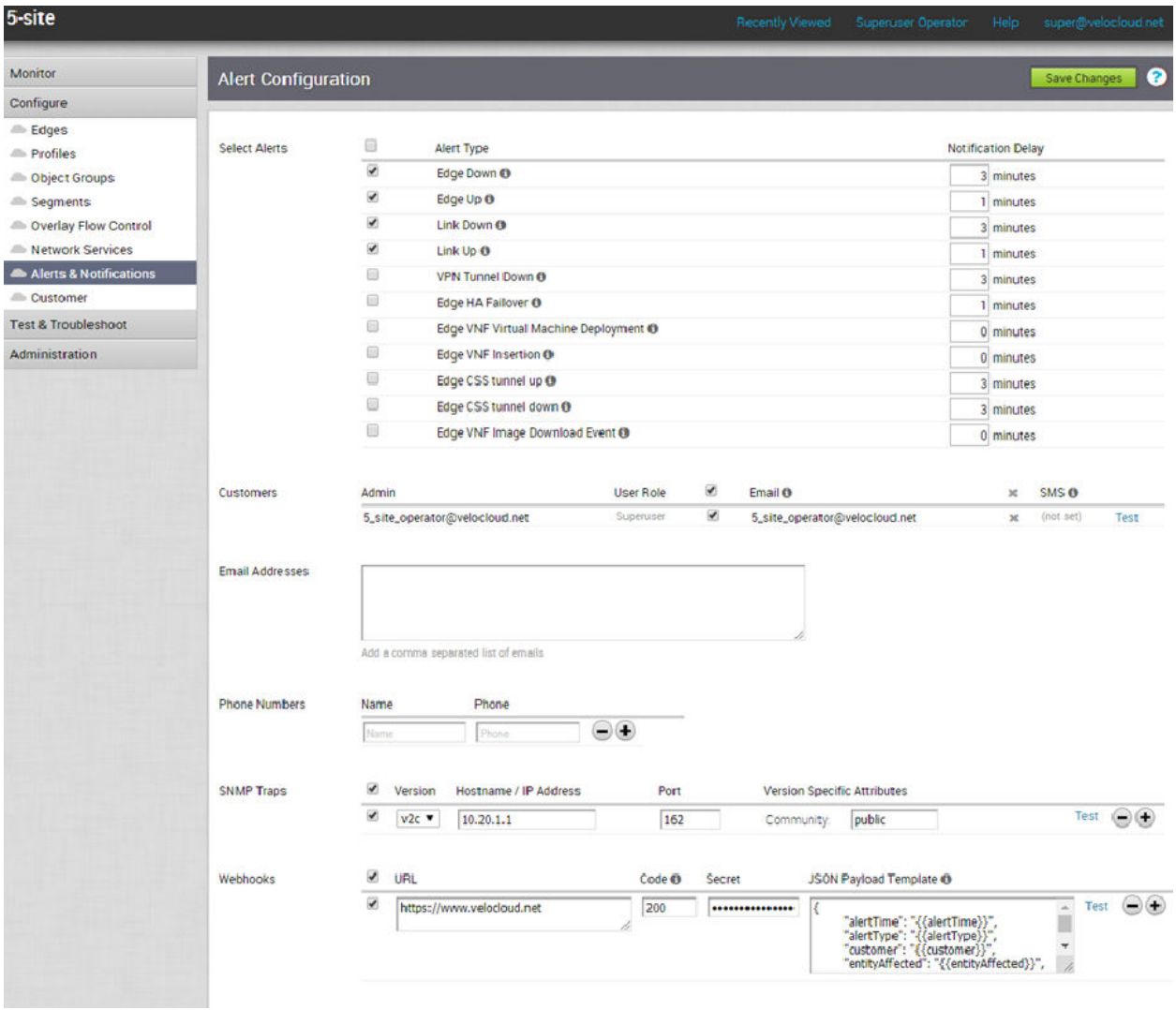
SD-WAN Orchestrator ermöglicht die Konfiguration von Warnungen, mit denen Unternehmensadministratoren oder andere Support-Benutzer benachrichtigt werden, wenn ein Ereignis eintritt.

Hinweis Wenn Sie als Benutzer mit Kunden-Support-Berechtigungen angemeldet sind, können Sie die Warnmeldungen und andere Objekte anzeigen, aber nicht konfigurieren.

Klicken Sie im Unternehmensportal auf **Konfigurieren (Configure) > Warnungen und Benachrichtigungen (Alerts & Notifications)**, um die Warnungen zu konfigurieren.

Wählen Sie die Ereignisse aus, für die die Warnungen gesendet werden sollen, und geben Sie unter **Warnungen auswählen (Select Alerts)** die Benachrichtigungsverzögerungszeit in Minuten ein.

Sie können das Ereignis `EDIT_ALERT_CONFIGURATION` verwenden, um die Änderungen an den Konfigurationen von Unternehmenswarnungen aufzuzeichnen.



Unter **Kunden (Customers)** werden die Kontaktdetails der vorhandenen Admin-Benutzer angezeigt. Sie können die Kontrollkästchen für E-Mail und SMS aktivieren, um Warnungen an die entsprechenden Benutzer zu senden.

SNMP-Traps (SNMP Traps)

SNMP (Simple Network Management Protocol)-Traps sind Benachrichtigungen, die an einen SNMP-Agenten gesendet werden, um anzugeben, dass ein Ereignis aufgetreten ist. SD-WAN Orchestrator sendet SNMP-Traps, die den vorhandenen Warnungen entsprechen, wie zum Beispiel „Edge nicht aktiv (Edge Down)“ oder „Edge aktiv (Edge Up)“. Sie können die SNMP-Version auswählen und die entsprechenden Details unter **SNMP-Traps (SNMP Traps)** eingeben.

Webhooks

Webhooks liefern Daten an andere Anwendungen, die von bestimmten Ereignissen mithilfe von HTTP POST ausgelöst werden. Wenn ein Ereignis eintritt, sendet die Quelle eine HTTP-Anfrage an die zielseitige Anwendung, die für den Webhook konfiguriert ist.

SD-WAN Orchestrator unterstützt Webhooks, die automatisch Nachrichten über HTTP POST an zielseitige Anwendungen senden, wenn ein Ereignis eintritt. Sie können die Ziel-URL im Unternehmensportal festlegen und Aktionen als Reaktion auf die von SD-WAN Orchestrator ausgelösten Warnungen automatisieren. Die Webhook-Empfänger müssen HTTPS unterstützen und über gültige Zertifikate verfügen, um den Datenschutz potenziell sensibler Warnungsnutzlasten zu gewährleisten. Dadurch wird auch verhindert, dass Nutzlasten manipuliert werden.

Webhooks konfigurieren (Configure Webhooks)

Im Fenster **Warnungskonfiguration (Alert Configuration)** können Sie unter **Webhooks** die folgenden Details eingeben.

Option	Beschreibung
URL	Geben Sie eine gültige HTTPS-URL ein. Diese dient als Zielanwendung für die Webhooks.
Code	Geben Sie für jeden Webhook-Empfänger einen erwarteten HTTP-Antwortstatuscode ein. Standardmäßig erwartet die SD-WAN Orchestrator-Instanz, dass Webhook-Empfänger auf HTTP-POST-Anfragen mit einem Statuscode wie HTTP 200 antworten. Wenn die SD-WAN Orchestrator-Instanz einen unerwarteten Statuscode von einem Empfängerserver oder Proxyserver empfängt, geht sie davon aus, dass die Warnmeldung fehlgeschlagen ist, und generiert ein `ALERT_DELIVERY_FAILED`-Kundenereignis. Dieses Ereignis hilft zu erkennen, wenn ein Webhook-Empfangsserver möglicherweise nicht wie erwartet funktioniert.

Option	Beschreibung
Geheim (Secret)	Geben Sie für jeden konfigurierten Webhook-Empfänger ein geheimes Token an, das zur Berechnung eines HMAC-Werts für jede an den entsprechenden Empfänger gesendete Webhook-Anforderung verwendet wird. Der HMAC-Wert ist in einen `X-Webhook-Signature`-HTTP-Header mit einem Versionsparameter eingebettet, der den Signaturalgorithmus und einen Zeitstempel identifiziert. `X-Webhook-Signature: v=<signature-version>&t=<timestamp>&s=<hmac>` Der Empfänger interpretiert die Komponenten wie folgt: ■ `v`: Version des Algorithmus, der für die Erstellung der Signatur verwendet wird. Der einzige unterstützte Wert ist **1**. ■ `t`: Zeitraum-Zeitstempel auf Millisekundenpräzision, der dem Zeitpunkt entspricht, zu dem die Anforderung gesendet wird. ■ `s`: Von SD-WAN Orchestrator berechneter HMAC-Wert. Der HMAC-Wert wird wie folgt berechnet: `HMAC-SHA256(request-body + '.' + timestamp, secret)`. Die Nachricht, die zur Berechnung des HMAC-Werts verwendet wird, wird durch Verkettung des Anforderungstexts, einer einzelnen Periode und des Wertes des Zeitstempelparameters, der im Signaturkopf erscheint, gebildet. Der spezifische HMAC-Algorithmus, der zum Erstellen des Codes verwendet wird, lautet SHA256. Nach dem Empfang einer Webhook-Anforderung kann der abhörende Server die Authentizität der Anforderung überprüfen, indem er seine eigene HMAC-SHA256-Signatur nach demselben Algorithmus berechnet und die neu berechnete Signatur mit der von der SD-WAN Orchestrator-Instanz.
JSON-Nutzlastvorlage (JSON Payload Template)	Dies ist ein erforderliches Feld. SD-WAN Orchestrator liefert Benachrichtigungen an jeden Webhook-Empfänger über eine JSON-Nutzlast, die im Text einer ausgehenden HTTP-POST-Anforderung enthalten ist. SD-WAN Orchestrator generiert den Inhalt der Nutzlast dynamisch, da die Benachrichtigungen durch variable Interpolation gesendet werden. Die unterstützten Platzhaltervariablen in der benutzerkonfigurierten Nutzlastvorlage werden durch warnungsspezifische Werte ersetzt. Webhook-Nutzlastvorlagen unterstützen die folgenden Platzhaltervariablen: ■ **alertTime**: Zeitpunkt, zu dem die Warnung ausgelöst wurde. ■ **alertType**: Der Typ der Warnung, wie EDGE_DOWN, LINK_UP, VNF_VM_DEPLOYED. ■ **customer**: Name des Kunden, an den die Benachrichtigung gesendet wird.

Option	Beschreibung
	■ **entityAffected**: Name der Entität, wie Edge oder Link oder VNF, auf die die Warnung angewendet wird. ■ **lastContact**: Der Zeitpunkt, zu dem der betroffene Edge zuletzt mit der SD-WAN Orchestrator-Instanz kommuniziert hat. Dies gilt nur für die Edge-Warnungen. ■ **message**: Eine kurze Nachricht, die das Ereignis beschreibt, das die Warnung ausgelöst hat. ■ **VCO**: Hostname oder öffentliche IP-Adresse der SD-WAN Orchestrator-Instanz, von der die Benachrichtigung gesendet wird.

Das folgende Beispiel zeigt ein Beispiel einer JSON-Nutzlastvorlage:

```
{
     "alertTime": "{{alertTime}}",
     "alertType": "{{alertType}}",
     "customer": "{{customer}}",
     "entityAffected": "{{entityAffected}}",
     "lastContact": "{{lastContact}}",
     "message": "{{message}}",
     "vco": "{{vco}}"
}
```

Sie können auf das Pluszeichen (**+**) klicken, um weitere Ziel-URLs und die entsprechenden Details hinzuzufügen.

Klicken Sie auf **Testen (Test)**, um die Webhook-Warnungen zu prüfen.

Immer dann, wenn eine Warnung ausgelöst wird, wird eine Warnmeldung zusammen mit den relevanten Informationen an die Ziel-URL gesendet.

Testen und Fehlerbehebung

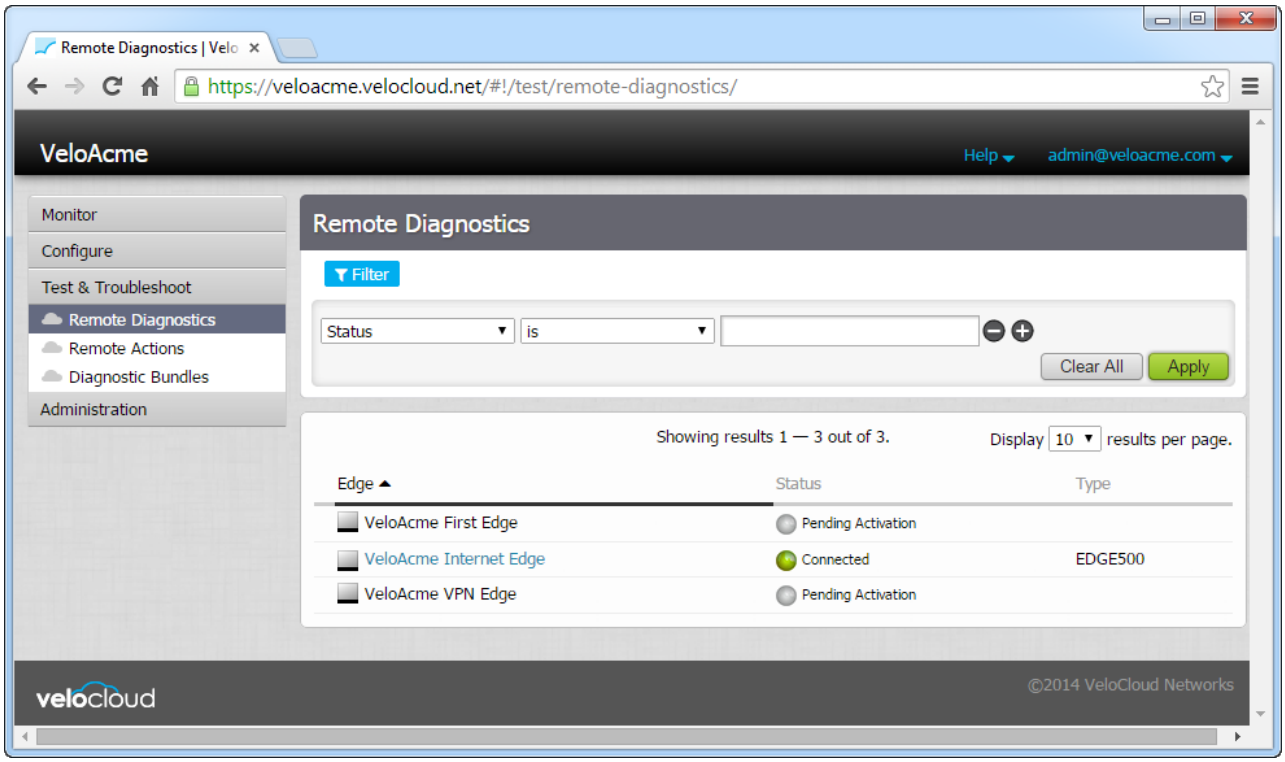
22

Die Funktion „Testen und Fehlerbehebung“ (Test & Troubleshoot) von SD-WAN Orchestrator bietet Tools zum Testen des Status des VMware SD-WAN-Diensts, zur Durchführung von Edge-Aktionen und zum Sammeln von Paketerfassungsinformationen für einen einzelnen Edge.

Sie können auf diese Funktionen im Abschnitt **Testen und Fehlerbehebung (Test & Troubleshoot)** des im folgenden aufgeführten Navigationsbereichs zugreifen:

- Remote-Diagnose
- Remote-Aktionen
- Diagnosepakete

Wenn Sie auf **Testen und Fehlerbehebung (Test & Troubleshoot)** klicken, wird der Bildschirm **Remote-Diagnose (Remote Diagnostics)** angezeigt. Er zeigt alle Edges an, die Sie in der Spalte **Edge** am unteren Rand des Bildschirms definiert haben.



Sie können den **Filter** verwenden, um Edges basierend auf dem Verbindungsstatus, dem Namen, der IP-Adresse, der Seriennummer, der Softwareversion und dem Software-Build zu finden. Bevor Sie jedoch die Maßnahmen im Bereich „Testen und Fehlerbehebung“ (Test & Troubleshoot) verwenden können, müssen Sie in der Spalte **Edge** einen Edge auswählen. Weitere Informationen zu den Optionen unter „Testen und Fehlerbehebung“ (Test & Troubleshoot), auf die Sie über den Navigationsbereich zugreifen können („Remote-Diagnose“ (Remote Diagnostics), „Remote-Aktionen“ (Remote Actions) und „Diagnosepakete“ (Diagnostic Bundles)) finden Sie in den folgenden Abschnitten.

Dieses Kapitel enthält die folgenden Themen:

- Remote-Diagnose
- Remote-Aktionen
- Diagnosepakete

Remote-Diagnose

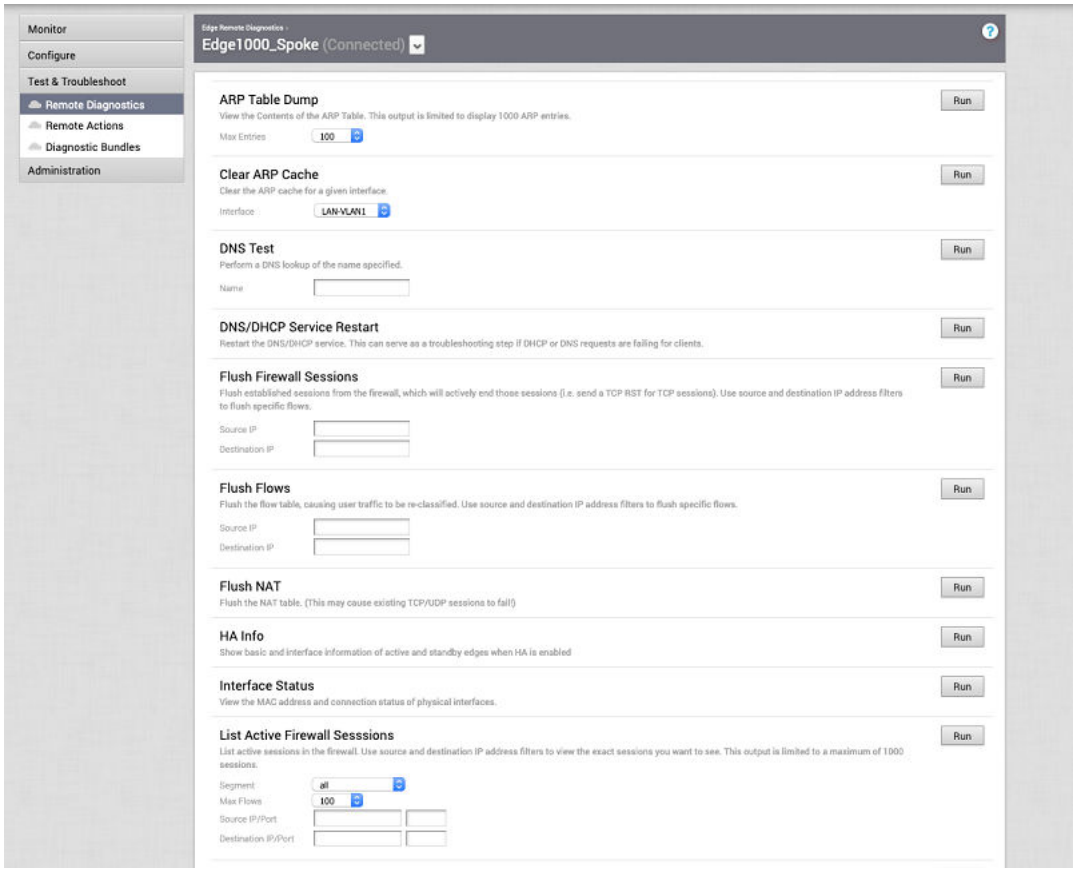
Sie können Tests auf einem Edge ausführen, um Diagnoseinformationen zu erhalten, indem Sie unter **Testen und Fehlerbehebung (Test & Troubleshoot)** auf **Remote-Diagnose (Remote Diagnostics)** klicken.

So führen Sie einen Diagnose-Test auf einem einzelnen Edge aus:

Verfahren

1. Klicken Sie im Unternehmensportal auf **Testen und Fehlerbehebung (Test & Troubleshoot)** und dann auf **Remote-Diagnose (Remote Diagnostic)**.
2. Suchen Sie bei Bedarf mit dem **Filter** nach einem Edge und klicken Sie dann auf **Anwenden (Apply)**.
3. Wählen Sie einen verbundenen Edge aus.

   Der Bildschirm **Remote-Diagnose (Remote Diagnostics)** wird mit allen möglichen Tests angezeigt, die Sie auf einem Edge ausführen können.



4 Wählen Sie einen Diagnose-Test aus, geben Sie die erforderlichen Details an und klicken Sie auf **Ausführen (Run)**.

Remote-Diagnosetests

Beschreibt alle möglichen Remote-Diagnosetests, die Sie auf einem Edge durchführen können, um Diagnosedaten zu erhalten. Die Diagnosedaten enthalten Edge-spezifische Protokolle für die Analyse.

Im Folgenden sind die unterstützen Remote-Diagnosetests aufgeführt:

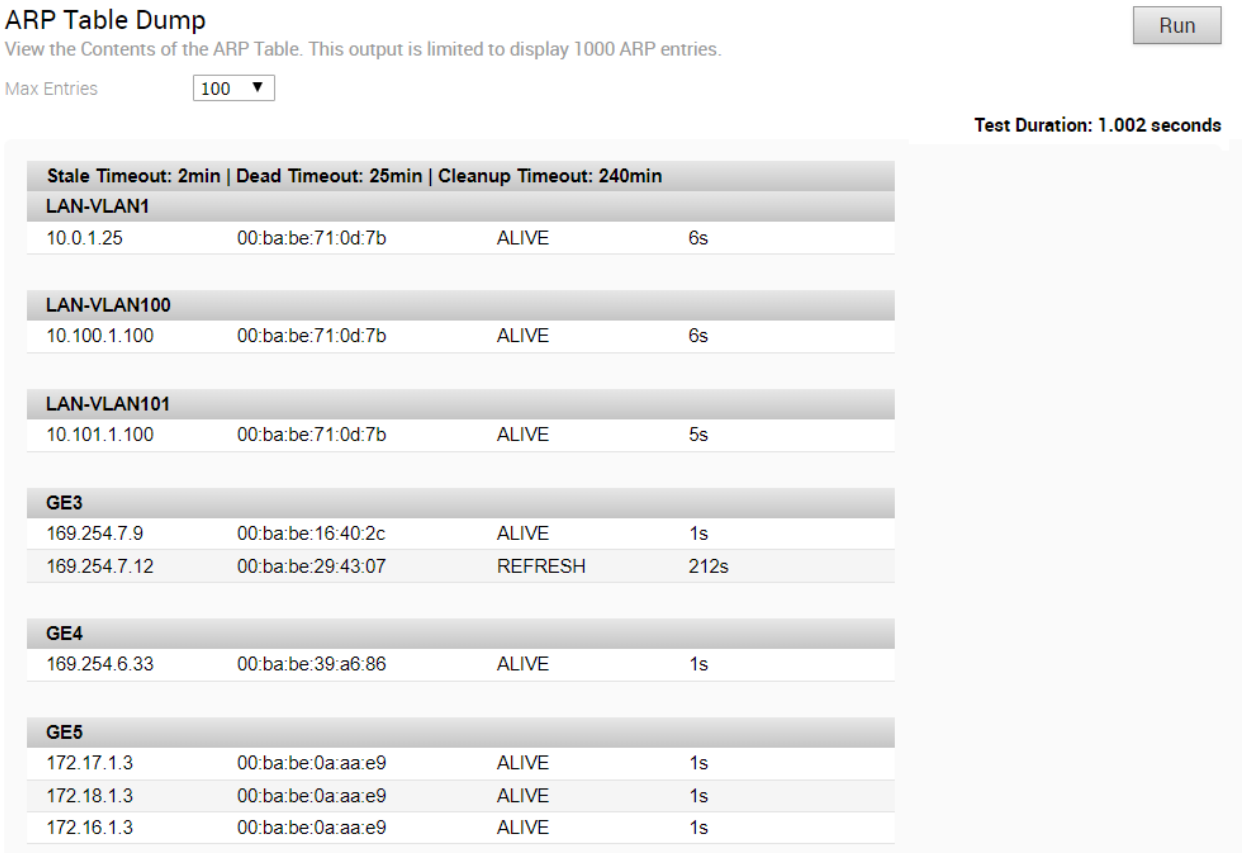
- ARP-Tabellenauszug (ARP Table Dump)
- ARP-Cache löschen (Clear ARP Cache)
- DNS-Test (DNS Test)
- Neustart des DNS/DHCP-Diensts (DNS/DHCP Service Restart)
- Firewallsitzungen leeren (Flush Firewall Sessions)
- Flows leeren (Flush Flows)
- NAT leeren (Flush NAT)
- Gateway
- Status der Schnittstelle

- Aktive Firewallsitzungen auflisten (List Active Firewall Sessions)
- Aktive Flows auflisten (List Active Flows)
- Clients auflisten (List Clients)
- Pfade auflisten (List Paths)
- MIBs für Edge (MIBs for Edge)
- NAT-Tabellenauszug (NAT Table Dump)
- NTP-Auszug (NTP Dump)
- Ping-Test (Ping Test)
- Auszug der Routentabelle (Route Table Dump)
- Systemzustand
- Traceroute
- Fehlerbehebung bei BGP – Umverteilte BGP-Routen auflisten (Troubleshoot BGP - List BGP Redistributed Routes)
- Fehlerbehebung bei BGP – BGP-Routen auflisten (Troubleshoot BGP - List BGP Routes)
- Fehlerbehebung bei BGP – Routen nach Präfix auflisten (Troubleshoot BGP - List Routes per Prefix)
- Fehlerbehebung bei BGP – Angekündigte BGP-Nachbar-Routen anzeigen (Troubleshoot BGP - Show BGP Neighbor Advertised Routes)
- Fehlerbehebung bei BGP – Gelernte BGP-Nachbar-Routen anzeigen (Troubleshoot BGP - Show BGP Neighbor Learned Routes)
- Fehlerbehebung bei BGP – Empfangene BGP-Nachbar-Routen anzeigen (Troubleshoot BGP - Show BGP Neighbor Received Routes)
- Fehlerbehebung bei BGP – BGP-Routen nach Präfix anzeigen (Troubleshoot BGP - Show BGP Routes per Prefix)
- Fehlerbehebung bei BGP – BGP-Übersicht anzeigen (Troubleshoot BGP - Show BGP Summary)
- Fehlerbehebung bei BGP – BGP-Tabelle anzeigen (Troubleshoot BGP - Show BGP Table)
- Fehlerbehebung bei OSPF – Umverteilte OSPF-Routen auflisten (Troubleshoot OSPF - List OSPF Redistributed Routes)
- Fehlerbehebung bei OSPF – OSPF-Routen auflisten (Troubleshoot OSPF - List OSPF Routes)
- Fehlerbehebung bei OSPF – OSPF-Datenbank anzeigen (Troubleshoot OSPF - Show OSPF Database)
- Fehlerbehebung bei OSPF – OSPF-Datenbank für E1-Self-Originate-Routen (Troubleshoot OSPF - Show OSPF Database for E1 Self-Originate Routes)

- Fehlerbehebung bei OSPF – OSPF-Nachbarn anzeigen (Troubleshoot OSPF - Show OSPF Neighbors)
- Fehlerbehebung bei OSPF – OSPF-Routentabelle anzeigen (Troubleshoot OSPF - Show OSPF Route Table)
- Fehlerbehebung bei OSPF – OSPF-Einstellung anzeigen (Troubleshoot OSPF - Show OSPF Setting)
- VPN-Test (VPN Test)
- Bandbreitentest für WAN-Link (WAN Link Bandwidth Test)

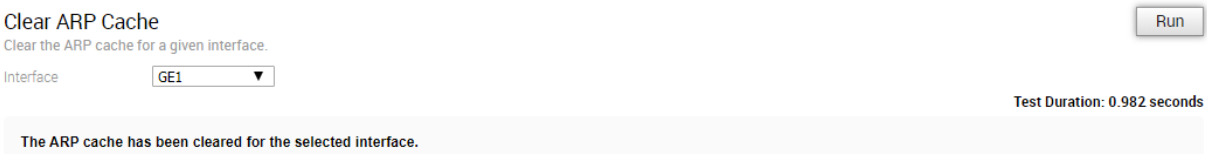
ARP-Tabellenauszug (ARP Table Dump)

Führen Sie diesen Test aus, um den Inhalt der Tabelle ARP-Tabelle anzuzeigen. Die Ausgabe ist auf 1.000 ARP-Einträge begrenzt.



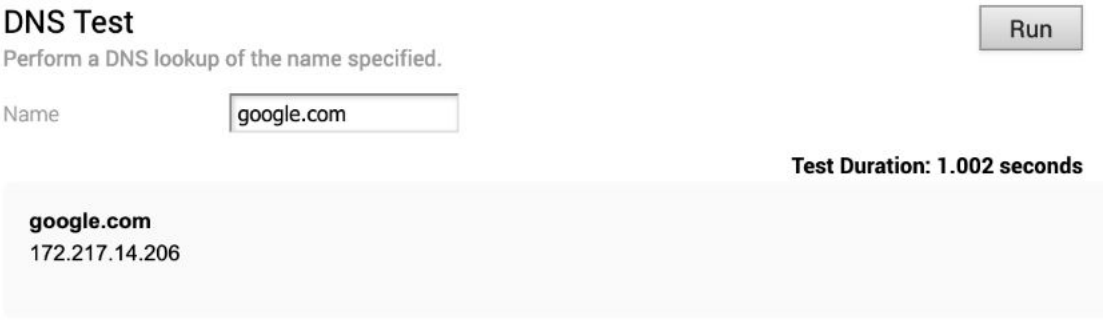
ARP-Cache löschen (Clear ARP Cache)

Führen Sie diesen Test aus, um die ARP-Cache-Einträge für die angegebene Schnittstelle zu löschen.



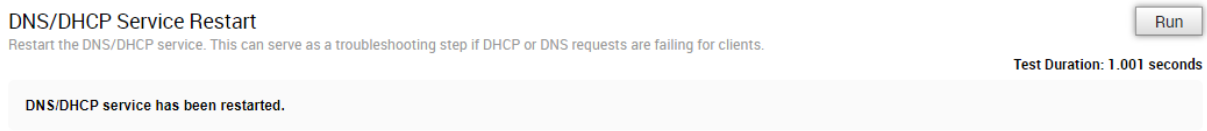
DNS-Test (DNS Test)

Führen Sie diesen Test aus, um eine DNS-Suche des angegebenen Domänennamens durchzuführen.



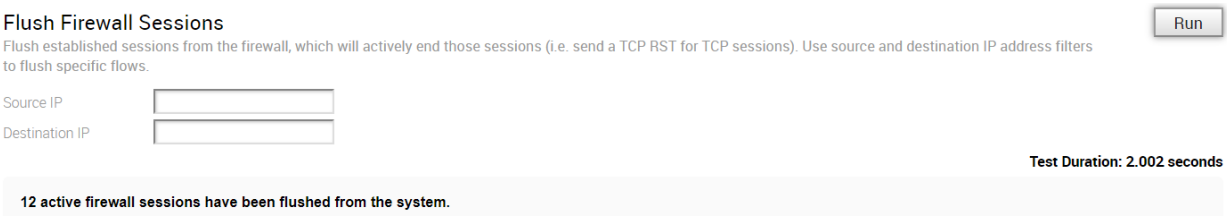
Neustart des DNS/DHCP-Diensts (DNS/DHCP Service Restart)

Führen Sie diesen Test aus, um den DNS/DHCP-Dienst neu zu starten. Dies kann als Fehlerbehebungsschritt dienen, wenn DHCP- oder DNS-Anfragen für Clients fehlschlagen.



Firewallsitzungen leeren (Flush Firewall Sessions)

Führen Sie diesen Test aus, um eingerichtete Sitzungen der Firewall zurückzusetzen. Wenn Sie diesen Test auf einem Edge ausführen, werden nicht nur die Firewallsitzungen geleert, sondern es wird auch aktiv ein TCP RST für die TCP-basierten Sitzungen gesendet.

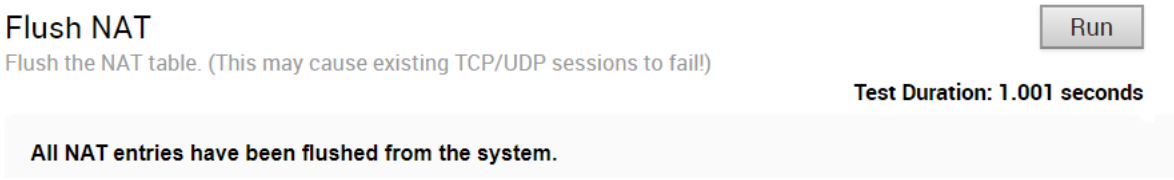


Flows leeren (Flush Flows)

Führen Sie diesen Test aus, um die Flow-Tabelle zu leeren, wodurch der Benutzerdatenverkehr neu klassifiziert wird. Verwenden Sie Filter für die Quell- und Ziel-IP-Adresse, um bestimmte Flows zu leeren.

NAT leeren (Flush NAT)

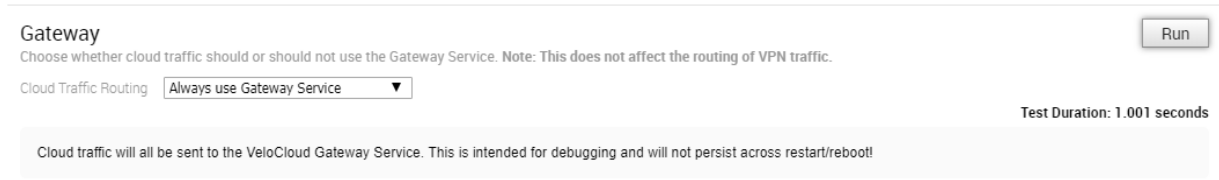
Führen Sie diesen Test aus, um die NAT-Tabelle zu leeren.



Gateway

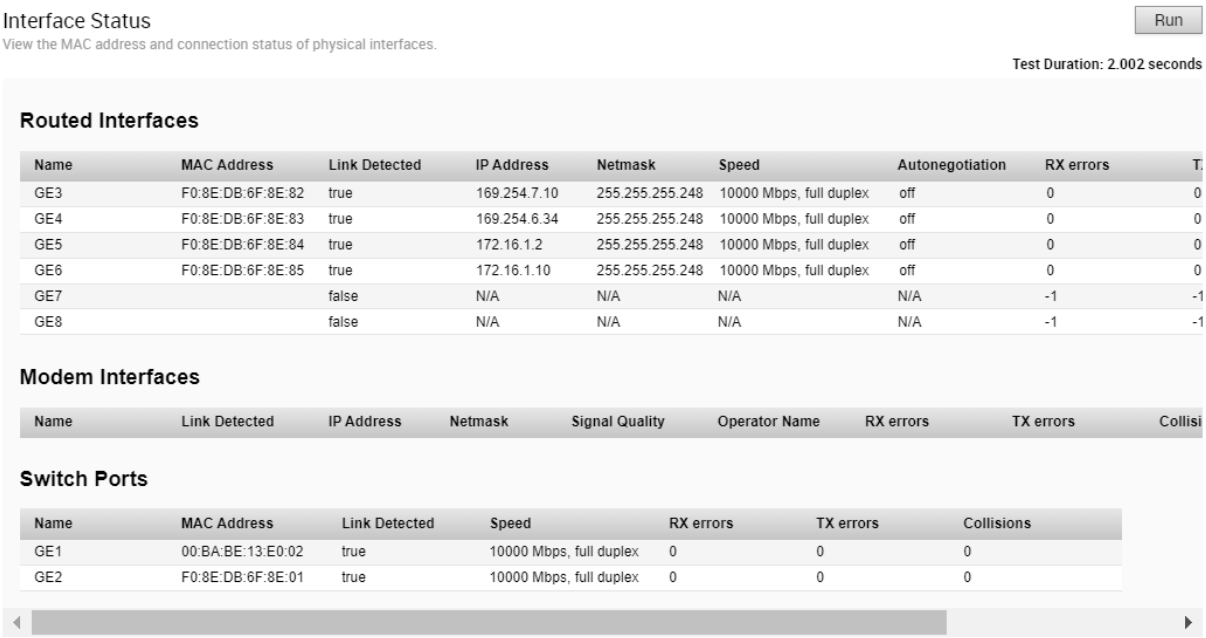
Führen Sie diesen Test aus, indem Sie auswählen, ob der Gateway-Dienst für Cloud-Datenverkehr verwendet werden soll oder nicht.

Hinweis Dies wirkt sich nicht auf das Routing des VPN-Datenverkehrs aus.



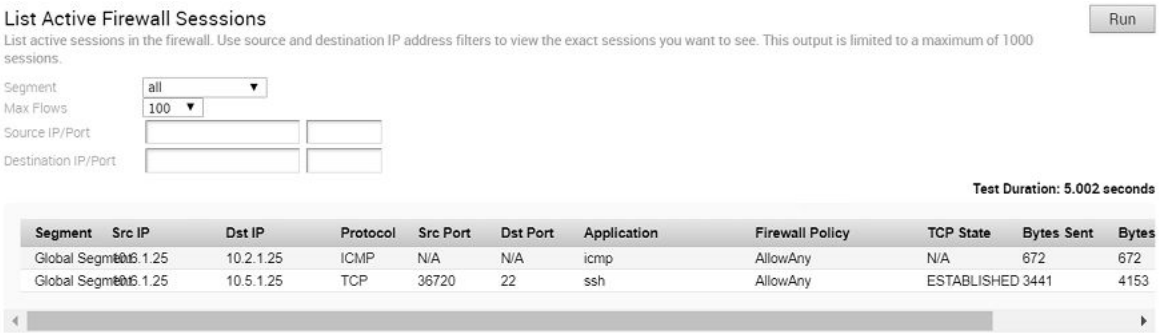
Status der Schnittstelle

Führen Sie diesen Test aus, um die MAC-Adresse und den Verbindungsstatus physischer Schnittstellen anzuzeigen.



Aktive Firewallsitzungen auflisten (List Active Firewall Sessions)

Führen Sie diesen Test aus, um den Status der aktiven Firewallsitzungen anzuzeigen (bis maximal 1.000 Sitzungen). Sie können die Anzahl der zurückgegebenen Sitzungen mithilfe von Filtern begrenzen: Quell- und Ziel-IP-Adresse, Quell- und Zielport sowie Segment.



Hinweis Es können keine Sitzungen angezeigt werden, die abgelehnt wurden, da es sich dabei nicht um aktive Sitzungen handelt. Zur Fehlerbehebung bei diesen Sitzungen müssen Sie die Firewallprotokolle überprüfen.

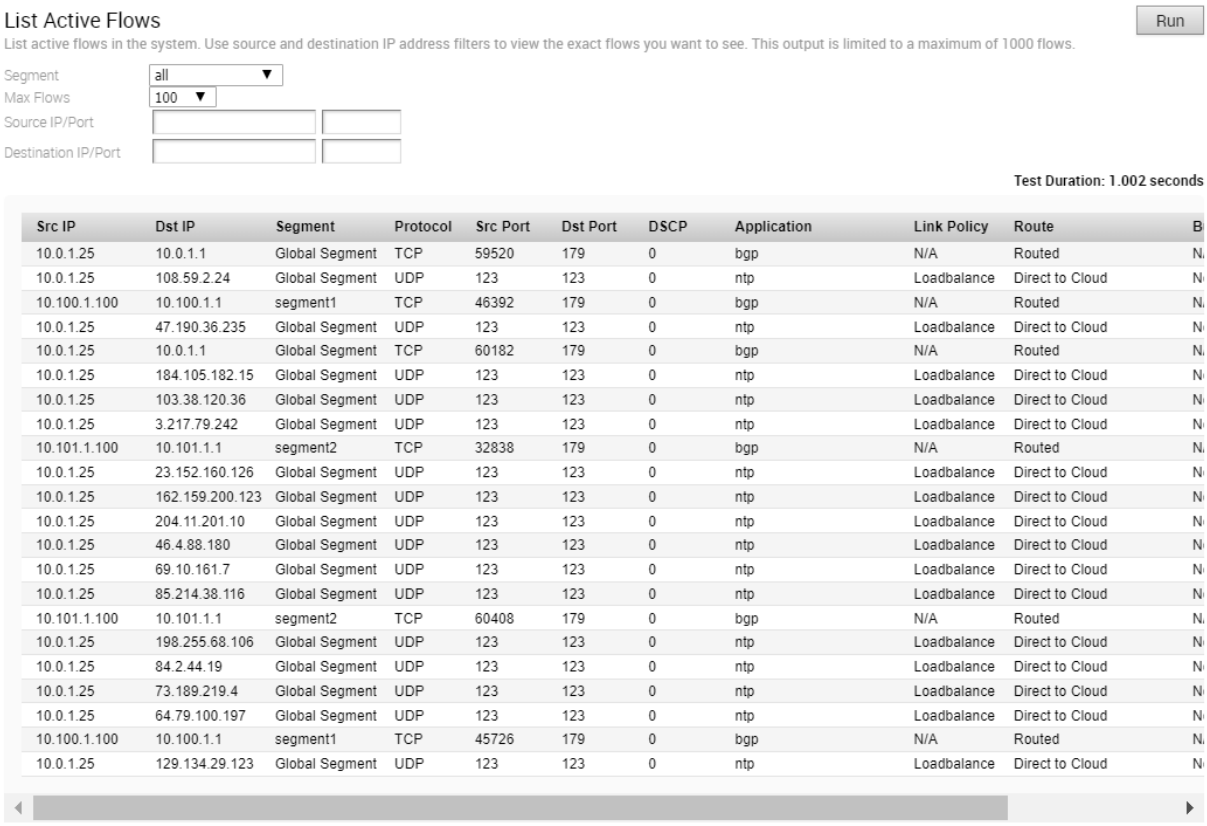
Die Ausgabe der Remotediagnose zeigt die folgenden Informationen an: Segmentname, Quell-IP, Quellport, Ziel-IP, Zielport, Protokoll, Anwendung, Firewallrichtlinie, aktueller TCP-Zustand ggf. vorhandener Flows, Empfangene/gesendete Byte und Dauer. Es gibt 11 eindeutige TCP-Zustände gemäß Definition in RFC 793:

- LISTEN: Steht für das Warten auf eine Verbindungsanforderung von einem beliebigen Remote-TCP und Port. (Dieser Zustand wird in einer Remote-Diagnoseausgabe nicht angezeigt.)

- SYN-SENT: Steht für das Warten auf eine passende Verbindungsanforderung, nachdem eine Verbindungsanforderung gesendet wurde.
- SYN-RECEIVED: Steht für das Warten auf die Bestätigung einer Verbindungsanforderung, nachdem eine Verbindungsanforderung gesendet und empfangen wurde.
- ESTABLISHED: Steht für eine offene Verbindung. Empfangene Daten können an den Benutzer übermittelt werden. Der normale Zustand für die Datenübertragungsphase der Verbindung.
- FIN-WAIT-1: Steht für das Warten auf eine Verbindungsabbruchanforderung vom Remote-TCP oder auf die Bestätigung einer zuvor gesendeten Verbindungsabbruchanforderung.
- FIN-WAIT-2: Steht für das Warten auf eine Verbindungsabbruchanforderung vom Remote-TCP.
- CLOSE-WAIT: Steht für das Warten auf eine Verbindungsabbruchanforderung vom lokalen Benutzer.
- CLOSING: Steht für das Warten auf die Bestätigung einer Verbindungsabbruchanforderung vom Remote-TCP.
- LAST-ACK: Steht für das Warten auf die Bestätigung einer Verbindungsabbruchanforderung, die zuvor an das Remote-TCP gesendet wurde (die schließt die Bestätigung der Verbindungsabbruchanforderung ein).
- TIME-WAIT: Steht für das Warten auf genügend Zeit, um sicherzustellen, dass das Remote-TCP die Bestätigung seiner Verbindungsabbruchanforderung erhalten hat.
- CLOSED: Steht für gar keinen Verbindungsstatus.

Aktive Flows auflisten (List Active Flows)

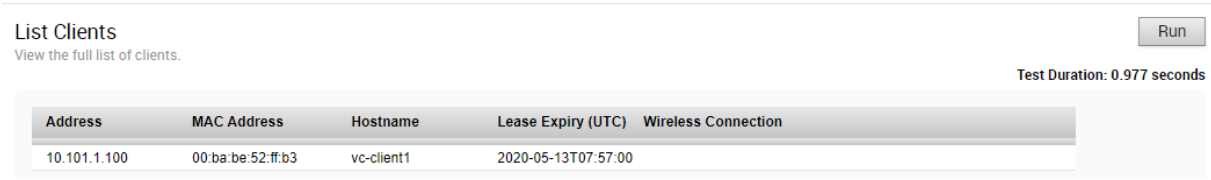
Führen Sie diesen Test aus, um aktive Flows im System aufzulisten. Verwenden Sie Filter für die Quell- und Ziel-IP-Adresse, um exakt die gewünschten Flows anzuzeigen. Diese Ausgabe ist auf maximal 1.000 Flows begrenzt.



Src IP	Dst IP	Segment	Protocol	Src Port	Dst Port	DSCP	Application	Link Policy	Route	B
10.0.1.25	10.0.1.1	Global Segment	TCP	59520	179	0	bgp	N/A	Routed	N
10.0.1.25	108.59.2.24	Global Segment	UDP	123	123	0	ntp	Loadbalance	Direct to Cloud	N
10.100.1.100	10.100.1.1	segment1	TCP	46392	179	0	bgp	N/A	Routed	N
10.0.1.25	47.190.36.235	Global Segment	UDP	123	123	0	ntp	Loadbalance	Direct to Cloud	N
10.0.1.25	10.0.1.1	Global Segment	TCP	60182	179	0	bgp	N/A	Routed	N
10.0.1.25	184.105.182.15	Global Segment	UDP	123	123	0	ntp	Loadbalance	Direct to Cloud	N
10.0.1.25	103.38.120.36	Global Segment	UDP	123	123	0	ntp	Loadbalance	Direct to Cloud	N
10.0.1.25	3.217.79.242	Global Segment	UDP	123	123	0	ntp	Loadbalance	Direct to Cloud	N
10.101.1.100	10.101.1.1	segment2	TCP	32838	179	0	bgp	N/A	Routed	N
10.0.1.25	23.152.160.126	Global Segment	UDP	123	123	0	ntp	Loadbalance	Direct to Cloud	N
10.0.1.25	162.159.200.123	Global Segment	UDP	123	123	0	ntp	Loadbalance	Direct to Cloud	N
10.0.1.25	204.11.201.10	Global Segment	UDP	123	123	0	ntp	Loadbalance	Direct to Cloud	N
10.0.1.25	46.4.88.180	Global Segment	UDP	123	123	0	ntp	Loadbalance	Direct to Cloud	N
10.0.1.25	69.10.161.7	Global Segment	UDP	123	123	0	ntp	Loadbalance	Direct to Cloud	N
10.0.1.25	85.214.38.116	Global Segment	UDP	123	123	0	ntp	Loadbalance	Direct to Cloud	N
10.101.1.100	10.101.1.1	segment2	TCP	60408	179	0	bgp	N/A	Routed	N
10.0.1.25	198.255.68.106	Global Segment	UDP	123	123	0	ntp	Loadbalance	Direct to Cloud	N
10.0.1.25	84.2.44.19	Global Segment	UDP	123	123	0	ntp	Loadbalance	Direct to Cloud	N
10.0.1.25	73.189.219.4	Global Segment	UDP	123	123	0	ntp	Loadbalance	Direct to Cloud	N
10.0.1.25	64.79.100.197	Global Segment	UDP	123	123	0	ntp	Loadbalance	Direct to Cloud	N
10.100.1.100	10.100.1.1	segment1	TCP	45726	179	0	bgp	N/A	Routed	N
10.0.1.25	129.134.29.123	Global Segment	UDP	123	123	0	ntp	Loadbalance	Direct to Cloud	N

Clients auflisten (List Clients)

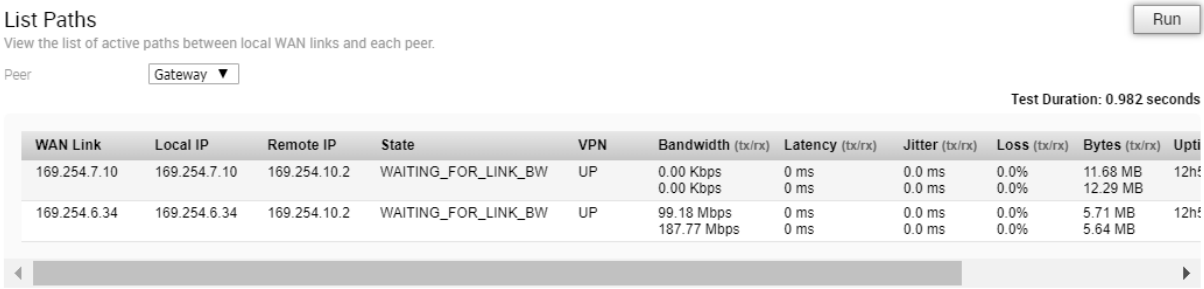
Führen Sie diesen Test aus, um die vollständige Liste der Clients anzuzeigen.



Address	MAC Address	Hostname	Lease Expiry (UTC)	Wireless Connection
10.101.1.100	00:ba:be:52:ff:b3	vc-client1	2020-05-13T07:57:00	

Pfade auflisten (List Paths)

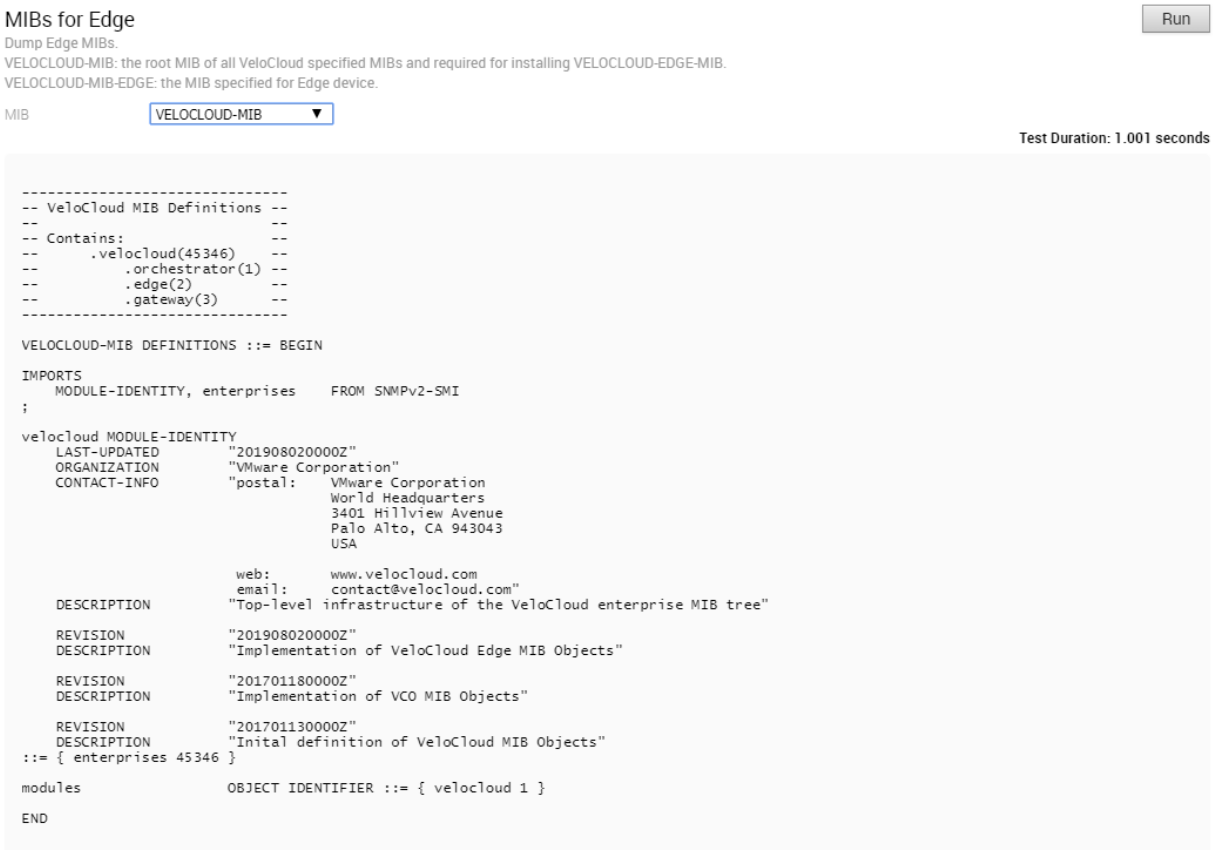
Führen Sie diesen Test aus, um die Liste der aktiven Pfade zwischen lokalen WAN-Links und jedem Peer anzuzeigen.



WAN Link	Local IP	Remote IP	State	VPN	Bandwidth (tx/rx)	Latency (tx/rx)	Jitter (tx/rx)	Loss (tx/rx)	Bytes (tx/rx)	Upti
169.254.7.10	169.254.7.10	169.254.10.2	WAITING_FOR_LINK_BW	UP	0.00 Kbps 0.00 Kbps	0 ms 0 ms	0.0 ms 0.0 ms	0.0% 0.0%	11.68 MB 12.29 MB	12h
169.254.6.34	169.254.6.34	169.254.10.2	WAITING_FOR_LINK_BW	UP	99.18 Mbps 187.77 Mbps	0 ms 0 ms	0.0 ms 0.0 ms	0.0% 0.0%	5.71 MB 5.64 MB	12h

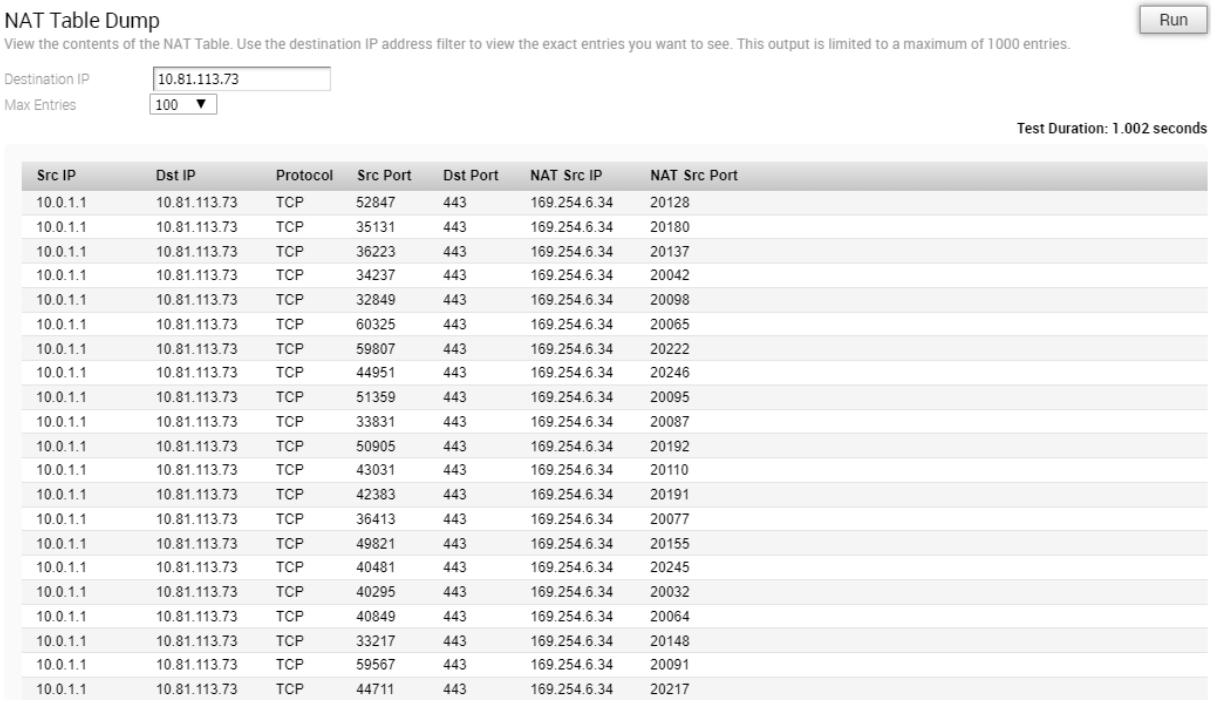
MIBs für Edge (MIBs for Edge)

Führen Sie diesen Test aus, um Edge-MIBs zu sichern.



NAT-Tabellenauszug (NAT Table Dump)

Führen Sie diesen Test aus, um den Inhalt der NAT-Tabelle anzuzeigen. Verwenden Sie den Filter für die Ziel-IP-Adresse, um exakt die gewünschten Einträge anzuzeigen. Diese Ausgabe ist auf maximal 1.000 Einträge begrenzt.



NAT Table Dump

View the contents of the NAT Table. Use the destination IP address filter to view the exact entries you want to see. This output is limited to a maximum of 1000 entries.

Run

Destination IP 10.81.113.73

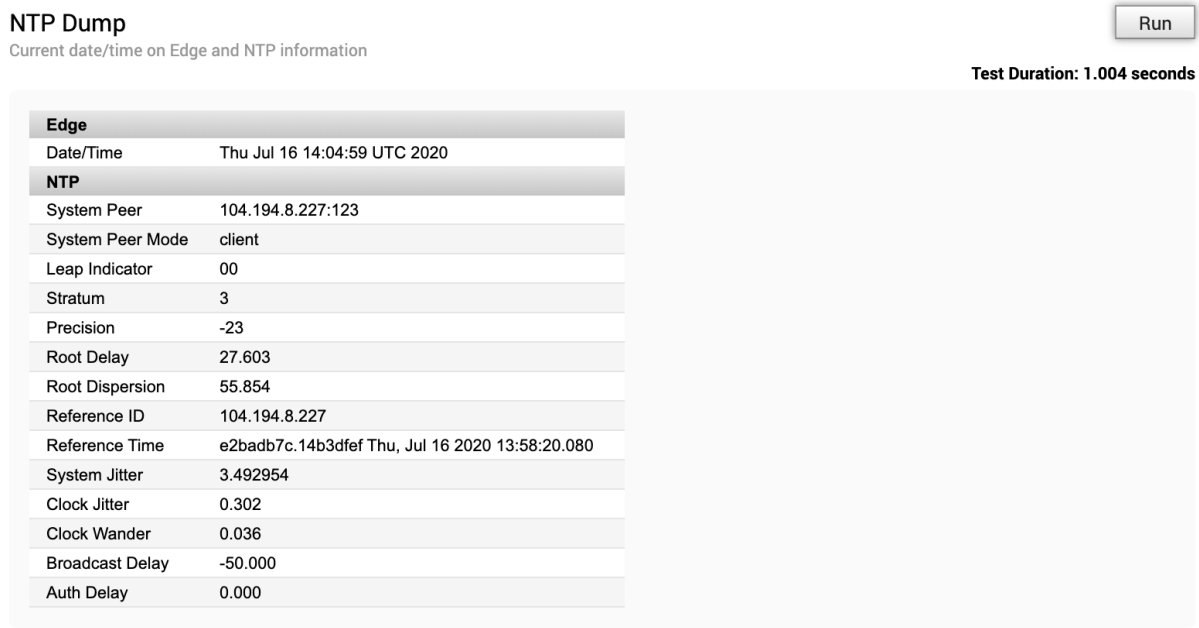
Max Entries 100

Test Duration: 1.002 seconds

Src IP	Dst IP	Protocol	Src Port	Dst Port	NAT Src IP	NAT Src Port
10.0.1.1	10.81.113.73	TCP	52847	443	169.254.6.34	20128
10.0.1.1	10.81.113.73	TCP	35131	443	169.254.6.34	20180
10.0.1.1	10.81.113.73	TCP	36223	443	169.254.6.34	20137
10.0.1.1	10.81.113.73	TCP	34237	443	169.254.6.34	20042
10.0.1.1	10.81.113.73	TCP	32849	443	169.254.6.34	20098
10.0.1.1	10.81.113.73	TCP	60325	443	169.254.6.34	20065
10.0.1.1	10.81.113.73	TCP	59807	443	169.254.6.34	20222
10.0.1.1	10.81.113.73	TCP	44951	443	169.254.6.34	20246
10.0.1.1	10.81.113.73	TCP	51359	443	169.254.6.34	20095
10.0.1.1	10.81.113.73	TCP	33831	443	169.254.6.34	20087
10.0.1.1	10.81.113.73	TCP	50905	443	169.254.6.34	20192
10.0.1.1	10.81.113.73	TCP	43031	443	169.254.6.34	20110
10.0.1.1	10.81.113.73	TCP	42383	443	169.254.6.34	20191
10.0.1.1	10.81.113.73	TCP	36413	443	169.254.6.34	20077
10.0.1.1	10.81.113.73	TCP	49821	443	169.254.6.34	20155
10.0.1.1	10.81.113.73	TCP	40481	443	169.254.6.34	20245
10.0.1.1	10.81.113.73	TCP	40295	443	169.254.6.34	20032
10.0.1.1	10.81.113.73	TCP	40849	443	169.254.6.34	20064
10.0.1.1	10.81.113.73	TCP	33217	443	169.254.6.34	20148
10.0.1.1	10.81.113.73	TCP	59567	443	169.254.6.34	20091
10.0.1.1	10.81.113.73	TCP	44711	443	169.254.6.34	20217

NTP-Auszug (NTP Dump)

Führen Sie diesen Test aus, um das aktuelle Datum und die aktuelle Uhrzeit für die Informationen zu Edge und NTP anzuzeigen.



NTP Dump

Current date/time on Edge and NTP information

Run

Test Duration: 1.004 seconds

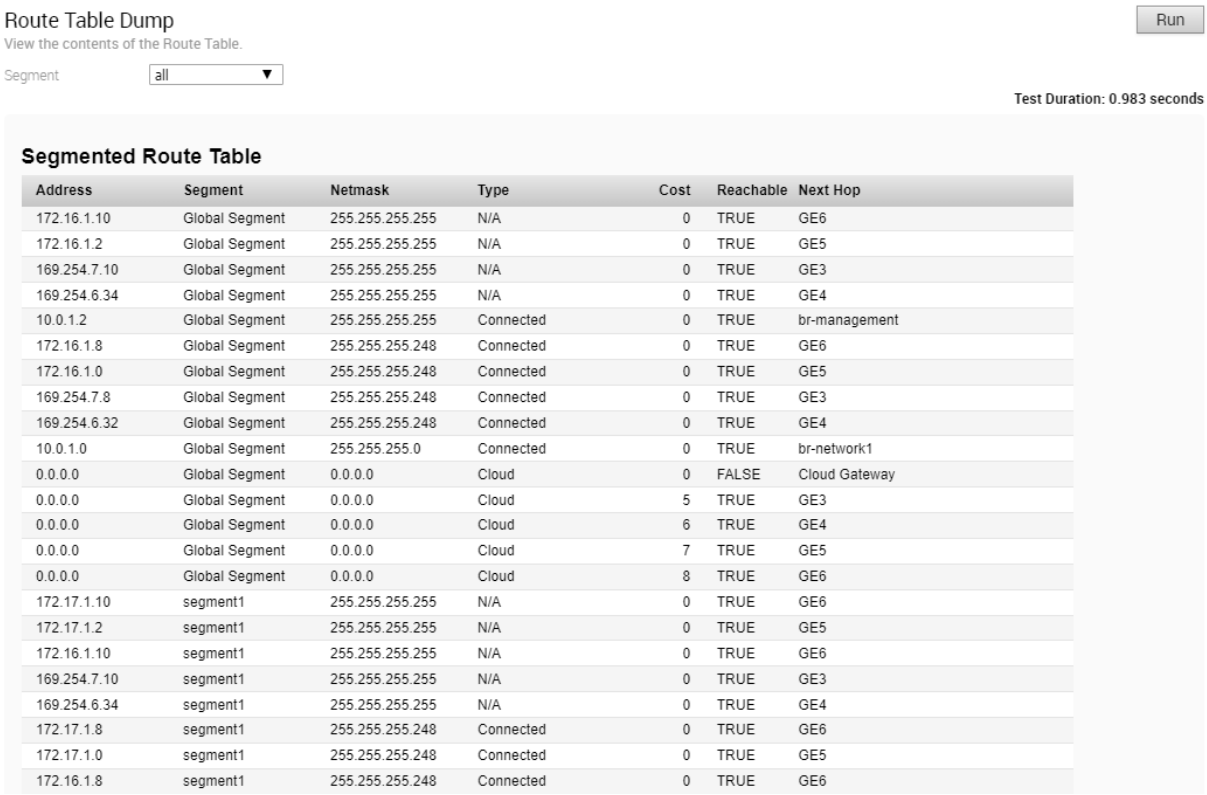
Edge	
Date/Time	Thu Jul 16 14:04:59 UTC 2020
NTP	
System Peer	104.194.8.227:123
System Peer Mode	client
Leap Indicator	00
Stratum	3
Precision	-23
Root Delay	27.603
Root Dispersion	55.854
Reference ID	104.194.8.227
Reference Time	e2badb7c.14b3dfef Thu, Jul 16 2020 13:58:20.080
System Jitter	3.492954
Clock Jitter	0.302
Clock Wander	0.036
Broadcast Delay	-50.000
Auth Delay	0.000

Ping-Test (Ping Test)

Führen Sie einen Ping-Test an das angegebene Ziel aus.

Auszug der Routentabelle (Route Table Dump)

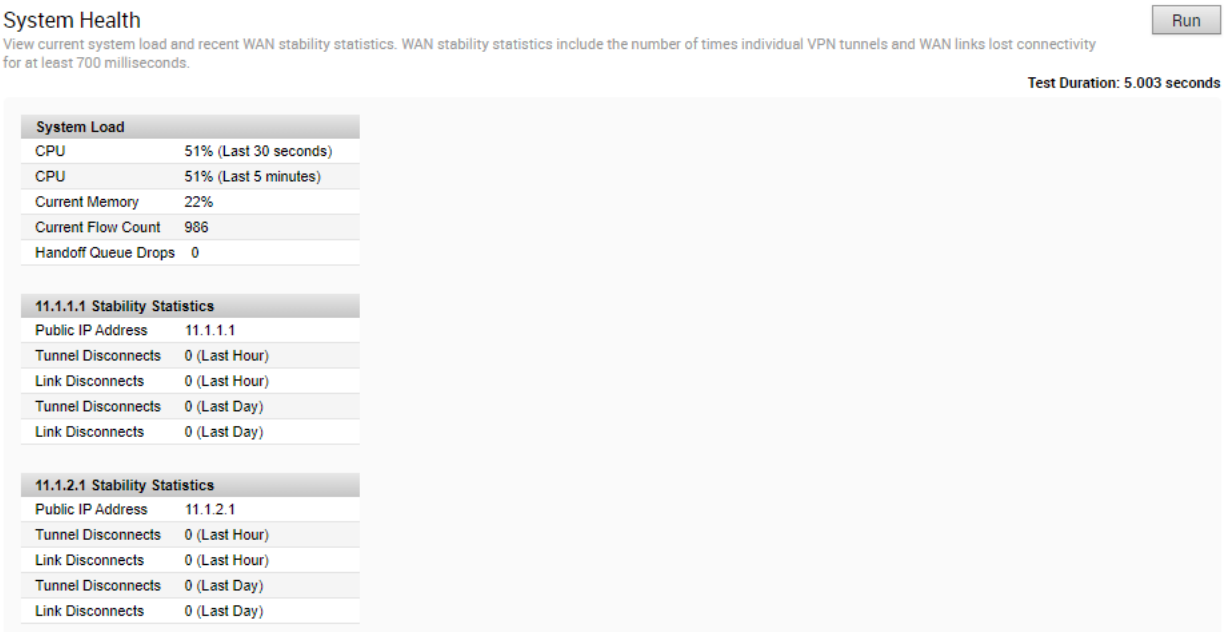
Führen Sie diesen Test aus, um den Inhalt der Routentabelle anzuzeigen.



Address	Segment	Netmask	Type	Cost	Reachable	Next Hop
172.16.1.10	Global Segment	255.255.255.255	N/A	0	TRUE	GE6
172.16.1.2	Global Segment	255.255.255.255	N/A	0	TRUE	GE5
169.254.7.10	Global Segment	255.255.255.255	N/A	0	TRUE	GE3
169.254.6.34	Global Segment	255.255.255.255	N/A	0	TRUE	GE4
10.0.1.2	Global Segment	255.255.255.255	Connected	0	TRUE	br-management
172.16.1.8	Global Segment	255.255.255.248	Connected	0	TRUE	GE6
172.16.1.0	Global Segment	255.255.255.248	Connected	0	TRUE	GE5
169.254.7.8	Global Segment	255.255.255.248	Connected	0	TRUE	GE3
169.254.6.32	Global Segment	255.255.255.248	Connected	0	TRUE	GE4
10.0.1.0	Global Segment	255.255.255.0	Connected	0	TRUE	br-network1
0.0.0.0	Global Segment	0.0.0.0	Cloud	0	FALSE	Cloud Gateway
0.0.0.0	Global Segment	0.0.0.0	Cloud	5	TRUE	GE3
0.0.0.0	Global Segment	0.0.0.0	Cloud	6	TRUE	GE4
0.0.0.0	Global Segment	0.0.0.0	Cloud	7	TRUE	GE5
0.0.0.0	Global Segment	0.0.0.0	Cloud	8	TRUE	GE6
172.17.1.10	segment1	255.255.255.255	N/A	0	TRUE	GE6
172.17.1.2	segment1	255.255.255.255	N/A	0	TRUE	GE5
172.16.1.10	segment1	255.255.255.255	N/A	0	TRUE	GE6
169.254.7.10	segment1	255.255.255.255	N/A	0	TRUE	GE3
169.254.6.34	segment1	255.255.255.255	N/A	0	TRUE	GE4
172.17.1.8	segment1	255.255.255.248	Connected	0	TRUE	GE6
172.17.1.0	segment1	255.255.255.248	Connected	0	TRUE	GE5
172.16.1.8	segment1	255.255.255.248	Connected	0	TRUE	GE6

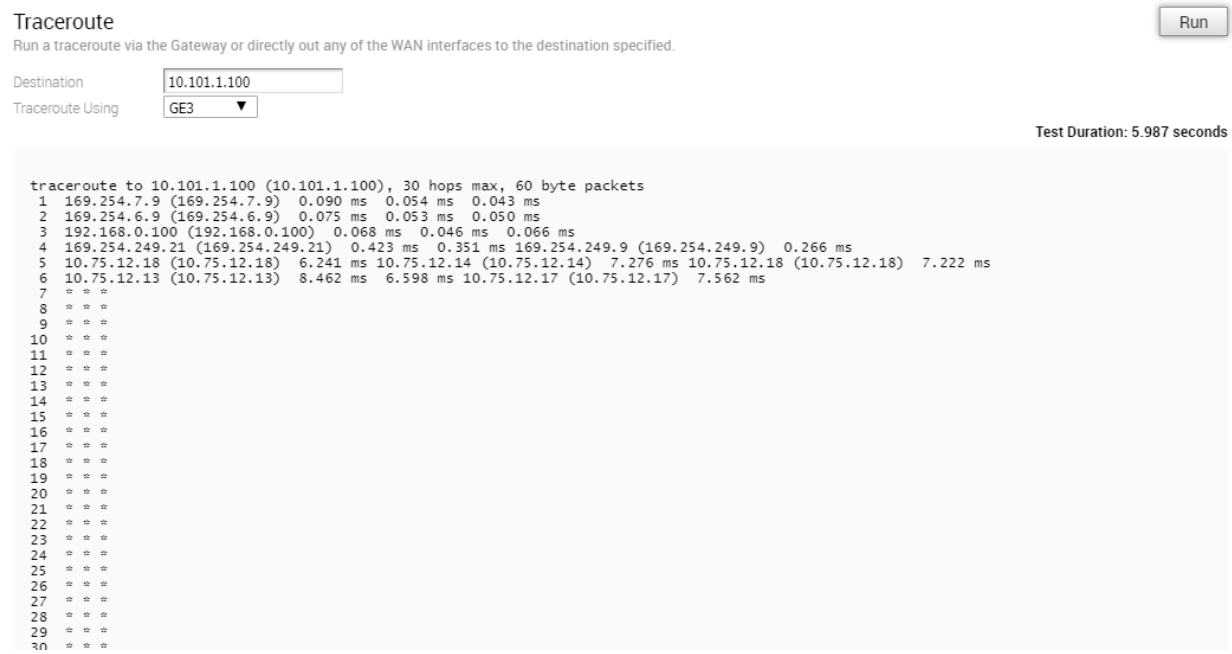
Systemzustand

Führen Sie diesen Test aus, um Systeminformationen wie z. B. die Systemlast, aktuelle Statistiken zur WAN-Stabilität und Überwachungsdienste anzuzeigen. Die WAN-Stabilitätsstatistiken umfassen die Angabe, wie oft die Verbindung mit einzelnen VPN-Tunneln und WAN-Links für mindestens 700 Millisekunden unterbrochen wurde.



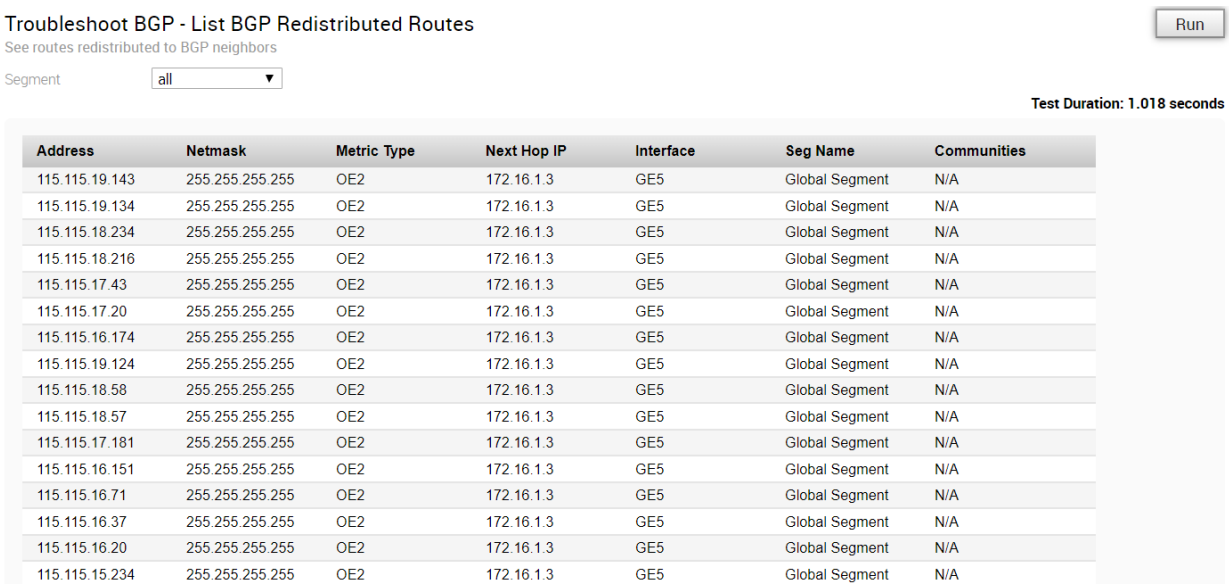
Traceroute

Führen Sie eine Traceroute über das Gateway oder direkt über eine der WAN-Schnittstellen zu dem angegebenen Ziel aus.



Fehlerbehebung bei BGP – Umverteilte BGP-Routen auflisten (Troubleshoot BGP - List BGP Redistributed Routes)

Führen Sie diesen Test aus, um die an BGP-Nachbarn umverteilten Routen anzuzeigen.



Troubleshoot BGP - List BGP Redistributed Routes

See routes redistributed to BGP neighbors

Run

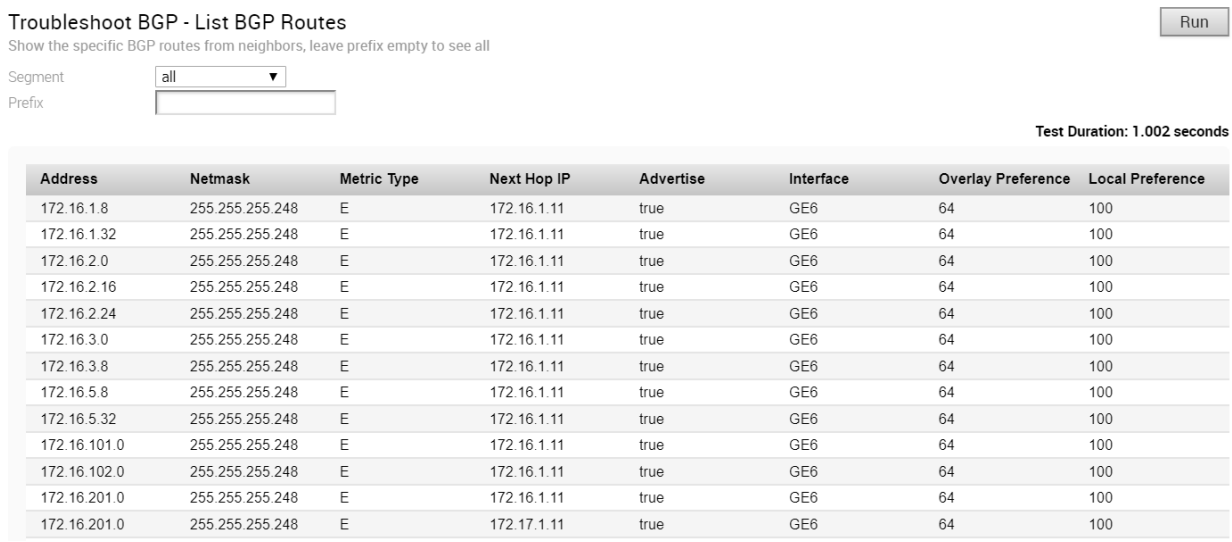
Segment: all

Test Duration: 1.018 seconds

Address	Netmask	Metric Type	Next Hop IP	Interface	Seg Name	Communities
115.115.19.143	255.255.255.255	OE2	172.16.1.3	GE5	Global Segment	N/A
115.115.19.134	255.255.255.255	OE2	172.16.1.3	GE5	Global Segment	N/A
115.115.18.234	255.255.255.255	OE2	172.16.1.3	GE5	Global Segment	N/A
115.115.18.216	255.255.255.255	OE2	172.16.1.3	GE5	Global Segment	N/A
115.115.17.43	255.255.255.255	OE2	172.16.1.3	GE5	Global Segment	N/A
115.115.17.20	255.255.255.255	OE2	172.16.1.3	GE5	Global Segment	N/A
115.115.16.174	255.255.255.255	OE2	172.16.1.3	GE5	Global Segment	N/A
115.115.19.124	255.255.255.255	OE2	172.16.1.3	GE5	Global Segment	N/A
115.115.18.58	255.255.255.255	OE2	172.16.1.3	GE5	Global Segment	N/A
115.115.18.57	255.255.255.255	OE2	172.16.1.3	GE5	Global Segment	N/A
115.115.17.181	255.255.255.255	OE2	172.16.1.3	GE5	Global Segment	N/A
115.115.16.151	255.255.255.255	OE2	172.16.1.3	GE5	Global Segment	N/A
115.115.16.71	255.255.255.255	OE2	172.16.1.3	GE5	Global Segment	N/A
115.115.16.37	255.255.255.255	OE2	172.16.1.3	GE5	Global Segment	N/A
115.115.16.20	255.255.255.255	OE2	172.16.1.3	GE5	Global Segment	N/A
115.115.15.234	255.255.255.255	OE2	172.16.1.3	GE5	Global Segment	N/A

Fehlerbehebung bei BGP – BGP-Routen auflisten (Troubleshoot BGP - List BGP Routes)

Führen Sie diesen Test aus, um die spezifischen BGP-Routen von Nachbarn anzuzeigen. Lassen Sie das Präfix leer, um alle anzuzeigen.



Troubleshoot BGP - List BGP Routes

Show the specific BGP routes from neighbors, leave prefix empty to see all

Run

Segment: all

Prefix:

Test Duration: 1.002 seconds

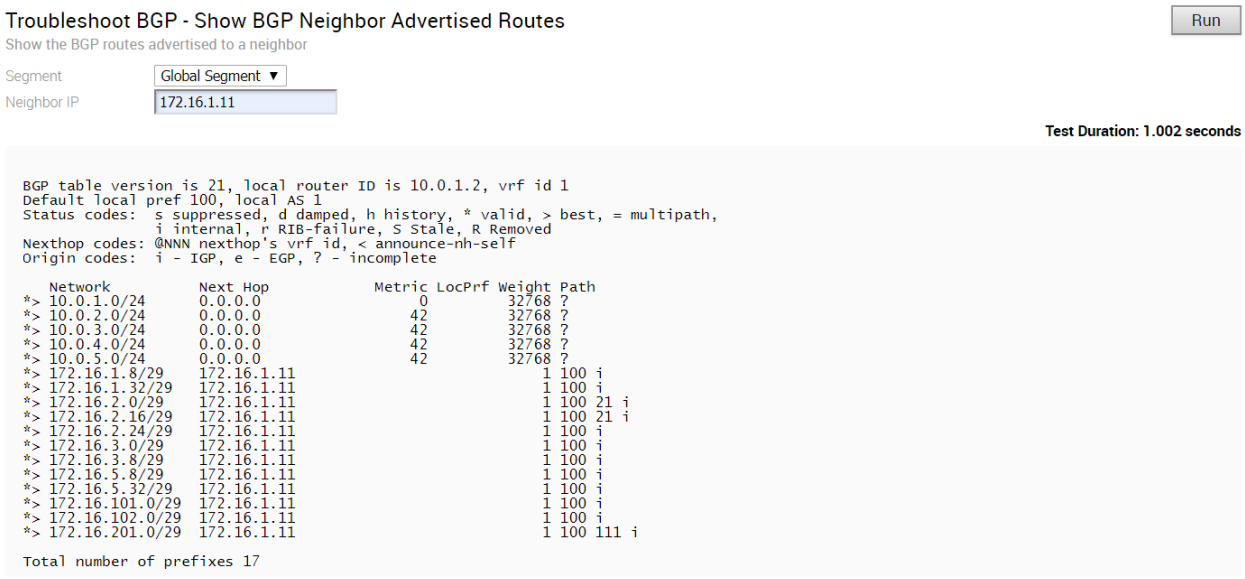
Address	Netmask	Metric Type	Next Hop IP	Advertise	Interface	Overlay Preference	Local Preference
172.16.1.8	255.255.255.248	E	172.16.1.11	true	GE6	64	100
172.16.1.32	255.255.255.248	E	172.16.1.11	true	GE6	64	100
172.16.2.0	255.255.255.248	E	172.16.1.11	true	GE6	64	100
172.16.2.16	255.255.255.248	E	172.16.1.11	true	GE6	64	100
172.16.2.24	255.255.255.248	E	172.16.1.11	true	GE6	64	100
172.16.3.0	255.255.255.248	E	172.16.1.11	true	GE6	64	100
172.16.3.8	255.255.255.248	E	172.16.1.11	true	GE6	64	100
172.16.5.8	255.255.255.248	E	172.16.1.11	true	GE6	64	100
172.16.5.32	255.255.255.248	E	172.16.1.11	true	GE6	64	100
172.16.101.0	255.255.255.248	E	172.16.1.11	true	GE6	64	100
172.16.102.0	255.255.255.248	E	172.16.1.11	true	GE6	64	100
172.16.201.0	255.255.255.248	E	172.16.1.11	true	GE6	64	100
172.16.201.0	255.255.255.248	E	172.17.1.11	true	GE6	64	100

Fehlerbehebung bei BGP – Routen nach Präfix auflisten (Troubleshoot BGP - List Routes per Prefix)

Führen Sie diesen Test aus, um alle Overlay- und Underlay-Routen für ein Präfix und die zugehörigen Details anzuzeigen.

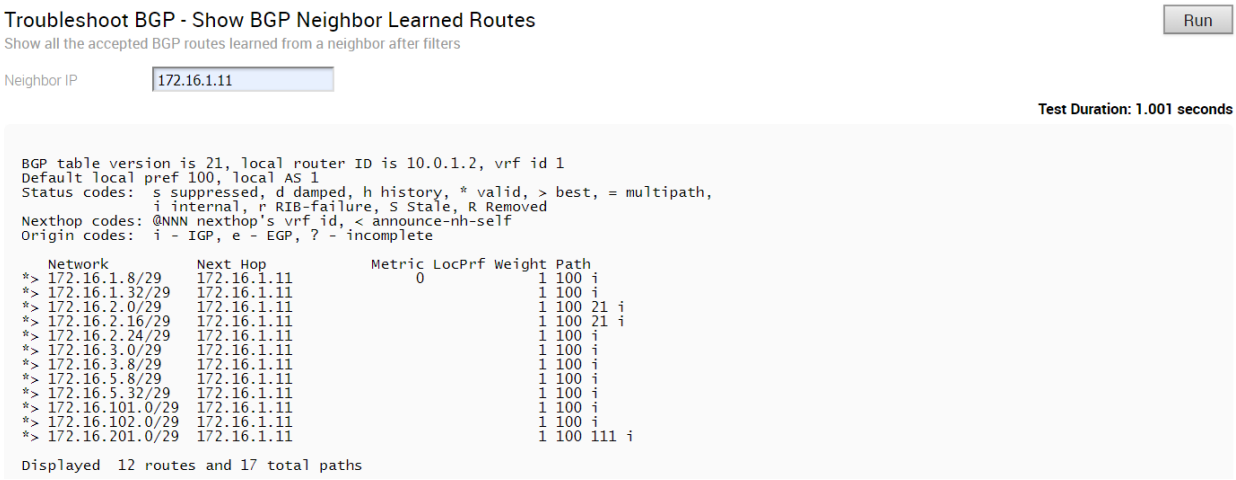
Fehlerbehebung bei BGP – Angekündigte BGP-Nachbar-Routen anzeigen (Troubleshoot BGP - Show BGP Neighbor Advertised Routes)

Führen Sie diesen Test aus, um die für einen Nachbarn angekündigten BGP-Routen anzuzeigen.



Fehlerbehebung bei BGP – Gelernte BGP-Nachbar-Routen anzeigen (Troubleshoot BGP - Show BGP Neighbor Learned Routes)

Führen Sie diesen Test aus, um alle von einem Nachbarn gelernten akzeptierten BGP-Routen nach Filtern anzuzeigen.

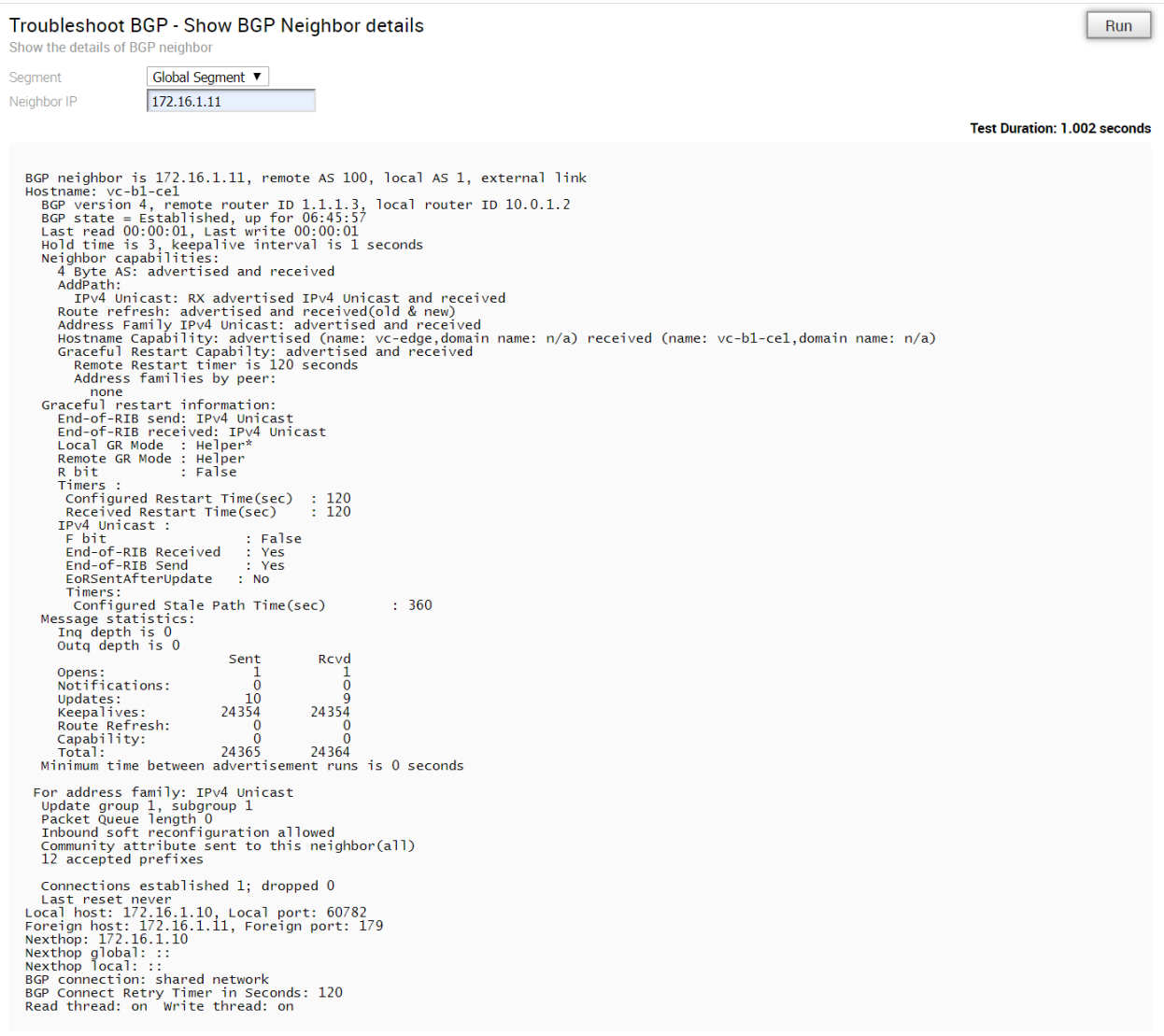


Fehlerbehebung bei BGP – Empfangene BGP-Nachbar-Routen anzeigen (Troubleshoot BGP - Show BGP Neighbor Received Routes)

Führen Sie diesen Test aus, um alle von einem Nachbarn gelernten BGP-Routen vor Filtern anzuzeigen.

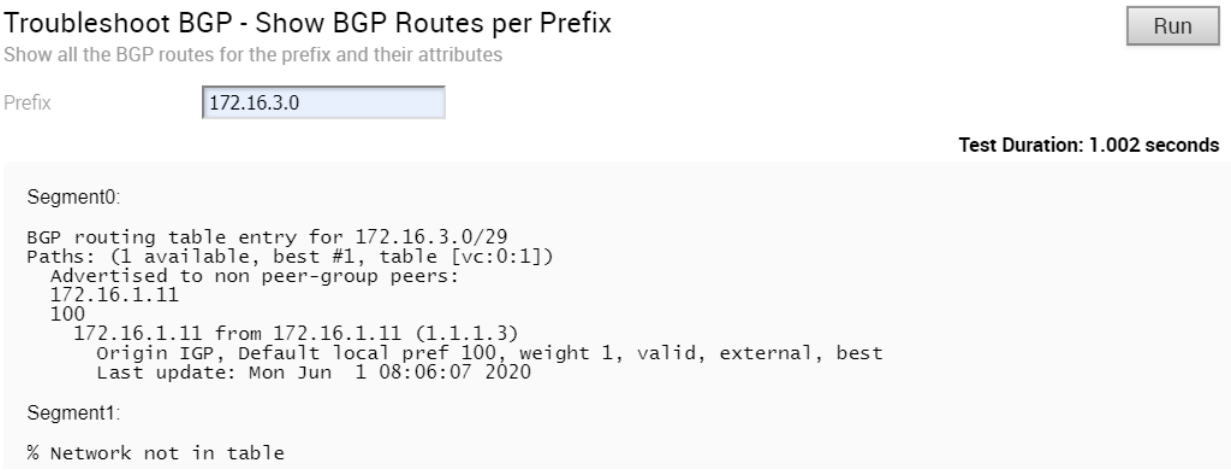
Fehlerbehebung bei BGP – Details zum BGP-Nachbarn anzeigen (Troubleshoot BGP - Show BGP Neighbor Details)

Führen Sie diesen Test aus, um die Details des BGP-Nachbarn anzuzeigen.



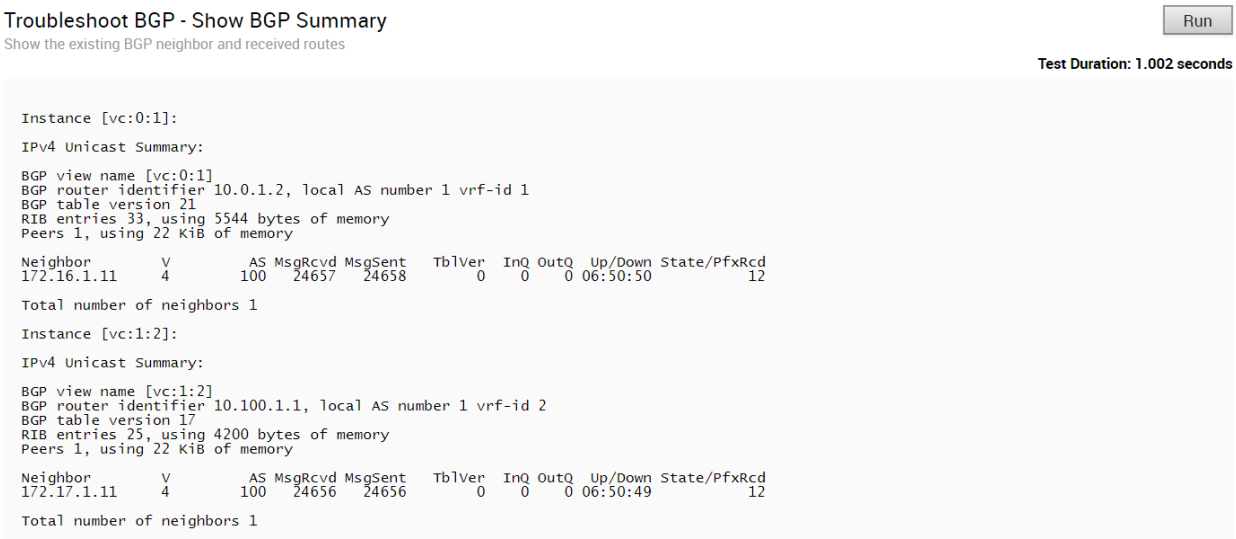
Fehlerbehebung bei BGP – BGP-Routen nach Präfix anzeigen (Troubleshoot BGP - Show BGP Routes per Prefix)

Führen Sie diesen Test aus, um alle BGP-Routen und ihre Attribute für das angegebene Präfix anzuzeigen.



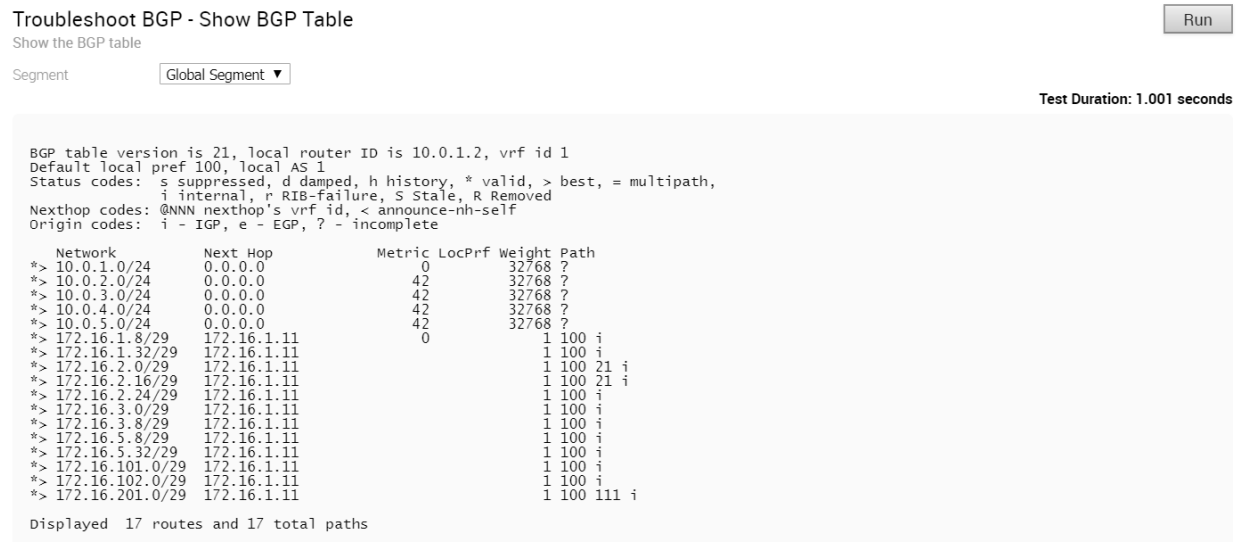
Fehlerbehebung bei BGP – BGP-Übersicht anzeigen (Troubleshoot BGP - Show BGP Summary)

Führen Sie diesen Test aus, um den vorhandenen BGP-Nachbarn und die empfangenen Routen anzuzeigen.



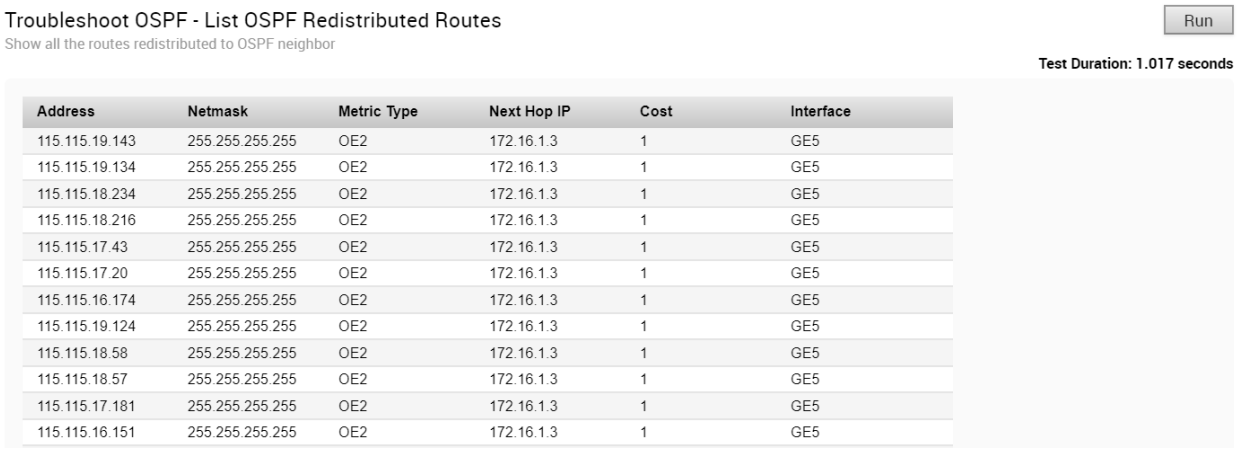
Fehlerbehebung bei BGP – BGP-Tabelle anzeigen (Troubleshoot BGP - Show BGP Table)

Führen Sie diesen Test aus, um die BGP-Tabelle anzuzeigen.



Fehlerbehebung bei OSPF – Umverteilte OSPF-Routen auflisten (Troubleshoot OSPF - List OSPF Redistributed Routes)

Führen Sie diesen Test aus, um alle an den OSPF-Nachbarn umverteilten Routen anzuzeigen.



Address	Netmask	Metric Type	Next Hop IP	Cost	Interface
115.115.19.143	255.255.255.255	OE2	172.16.1.3	1	GE5
115.115.19.134	255.255.255.255	OE2	172.16.1.3	1	GE5
115.115.18.234	255.255.255.255	OE2	172.16.1.3	1	GE5
115.115.18.216	255.255.255.255	OE2	172.16.1.3	1	GE5
115.115.17.43	255.255.255.255	OE2	172.16.1.3	1	GE5
115.115.17.20	255.255.255.255	OE2	172.16.1.3	1	GE5
115.115.16.174	255.255.255.255	OE2	172.16.1.3	1	GE5
115.115.19.124	255.255.255.255	OE2	172.16.1.3	1	GE5
115.115.18.58	255.255.255.255	OE2	172.16.1.3	1	GE5
115.115.18.57	255.255.255.255	OE2	172.16.1.3	1	GE5
115.115.17.181	255.255.255.255	OE2	172.16.1.3	1	GE5
115.115.16.151	255.255.255.255	OE2	172.16.1.3	1	GE5

Fehlerbehebung bei OSPF – OSPF-Routen auflisten (Troubleshoot OSPF - List OSPF Routes)

Führen Sie diesen Test aus, um die OSPF-Routen von Nachbarn für das angegebene Präfix anzuzeigen. Zeigt alle OSPF-Routen von Nachbarn an, wenn das Präfix nicht angegeben ist.

Troubleshoot OSPF - List OSPF Routes

Show the specific OSPF routes from neighbors, leave prefix empty to see all

Run

Prefix

Test Duration: 2.025 seconds

Address	Netmask	Metric Type	Nbr ID	OSPF Cost	Overlay Preference	Advertise	Interface
115.115.15.143	255.255.255.255	OE2	1.1.1.2	1	64	false	GE5
115.115.15.144	255.255.255.255	OE2	1.1.1.2	1	64	false	GE5
115.115.15.145	255.255.255.255	OE2	1.1.1.2	1	64	false	GE5
115.115.15.146	255.255.255.255	OE2	1.1.1.2	1	64	false	GE5
115.115.15.147	255.255.255.255	OE2	1.1.1.2	1	64	false	GE5
115.115.15.148	255.255.255.255	OE2	1.1.1.2	1	64	false	GE5
115.115.15.149	255.255.255.255	OE2	1.1.1.2	1	64	false	GE5
115.115.15.150	255.255.255.255	OE2	1.1.1.2	1	64	false	GE5
115.115.15.151	255.255.255.255	OE2	1.1.1.2	1	64	false	GE5
115.115.15.152	255.255.255.255	OE2	1.1.1.2	1	64	false	GE5
115.115.15.153	255.255.255.255	OE2	1.1.1.2	1	64	false	GE5
115.115.15.154	255.255.255.255	OE2	1.1.1.2	1	64	false	GE5
115.115.15.155	255.255.255.255	OE2	1.1.1.2	1	64	false	GE5

Fehlerbehebung bei OSPF – OSPF-Datenbank anzeigen (Troubleshoot OSPF - Show OSPF Database)

Führen Sie diesen Test aus, um die Zusammenfassung der OSPF-Verbindungsstatus-Datenbank anzuzeigen.

Troubleshoot OSPF - Show OSPF Database

Show the OSPF link state database summary

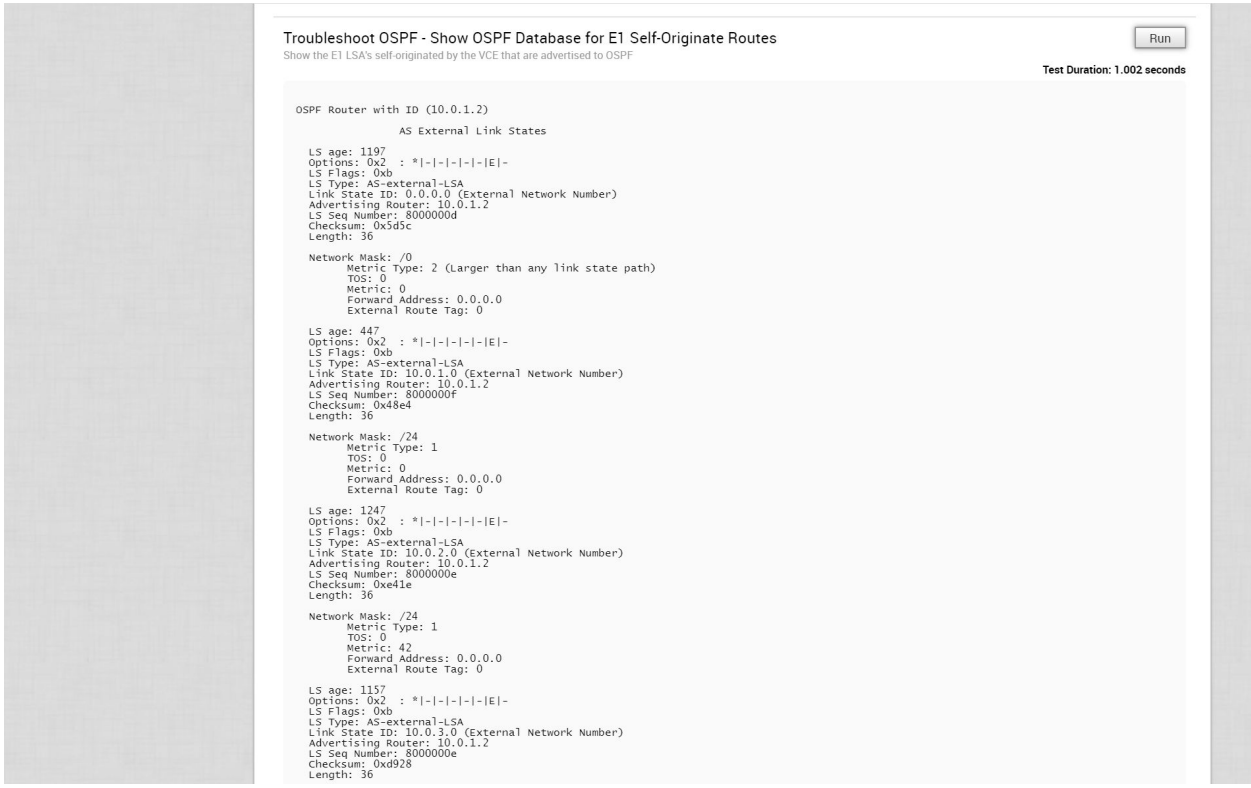
Run

Test Duration: 1.003 seconds

```
OSPF Router with ID (10.0.1.2)

                Router Link States (Area 0.0.0.1)

Link ID         ADV Router      Age  Seq#       CkSum  Link count
1.1.1.2         1.1.1.2         779 0x80000014 0x26a2 2
10.0.1.2        10.0.1.2       1015 0x8000000e 0x6049 1

                Net Link States (Area 0.0.0.1)

Link ID         ADV Router      Age  Seq#       CkSum
172.16.1.3      1.1.1.2        1039 0x8000000c 0x126c

                AS External Link States

Link ID         ADV Router      Age  Seq#       CkSum  Route
0.0.0.0         10.0.1.2       1055 0x8000000d 0x5d5c E2 0.0.0.0/0 [0x0]
10.0.1.0        10.0.1.2        305 0x8000000f 0x48e4 E1 10.0.1.0/24 [0x0]
10.0.2.0        10.0.1.2       1105 0x8000000e 0xe41e E1 10.0.2.0/24 [0x0]
10.0.3.0        10.0.1.2       1015 0x8000000e 0xd928 E1 10.0.3.0/24 [0x0]
10.0.4.0        10.0.1.2       1025 0x8000000e 0xce32 E1 10.0.4.0/24 [0x0]
10.0.5.0        10.0.1.2       1025 0x8000000e 0xc33c E1 10.0.5.0/24 [0x0]
115.115.15.143  1.1.1.2         749 0x8000000c 0xe93f E2 115.115.15.143/32 [0x0]
115.115.15.144  1.1.1.2         909 0x8000000c 0xdf48 E2 115.115.15.144/32 [0x0]
115.115.15.145  1.1.1.2         849 0x8000000c 0xd551 E2 115.115.15.145/32 [0x0]
115.115.15.146  1.1.1.2         889 0x8000000c 0xcb5a E2 115.115.15.146/32 [0x0]
115.115.15.147  1.1.1.2         779 0x8000000c 0xc163 E2 115.115.15.147/32 [0x0]
115.115.15.148  1.1.1.2         859 0x8000000c 0xb76c E2 115.115.15.148/32 [0x0]
115.115.15.149  1.1.1.2         869 0x8000000c 0xad75 E2 115.115.15.149/32 [0x0]
115.115.15.150  1.1.1.2         799 0x8000000c 0xa37e E2 115.115.15.150/32 [0x0]
115.115.15.151  1.1.1.2         829 0x8000000c 0x9987 E2 115.115.15.151/32 [0x0]
115.115.15.152  1.1.1.2         839 0x8000000c 0x8f90 E2 115.115.15.152/32 [0x0]
115.115.15.153  1.1.1.2         869 0x8000000c 0x8599 E2 115.115.15.153/32 [0x0]
115.115.15.154  1.1.1.2         789 0x8000000c 0x7ba2 E2 115.115.15.154/32 [0x0]
115.115.15.155  1.1.1.2         779 0x8000000c 0x71ab E2 115.115.15.155/32 [0x0]
```

Fehlerbehebung bei OSPF – OSPF-Datenbank für E1-Self-Originate-Routen (Troubleshoot OSPF - Show OSPF Database for E1 Self-Originate Routes)

Führen Sie diesen Test aus, um die selbst erstellten E1 LSA-Routen anzuzeigen, die OSPF-Routern vom Edge angekündigt wurden.

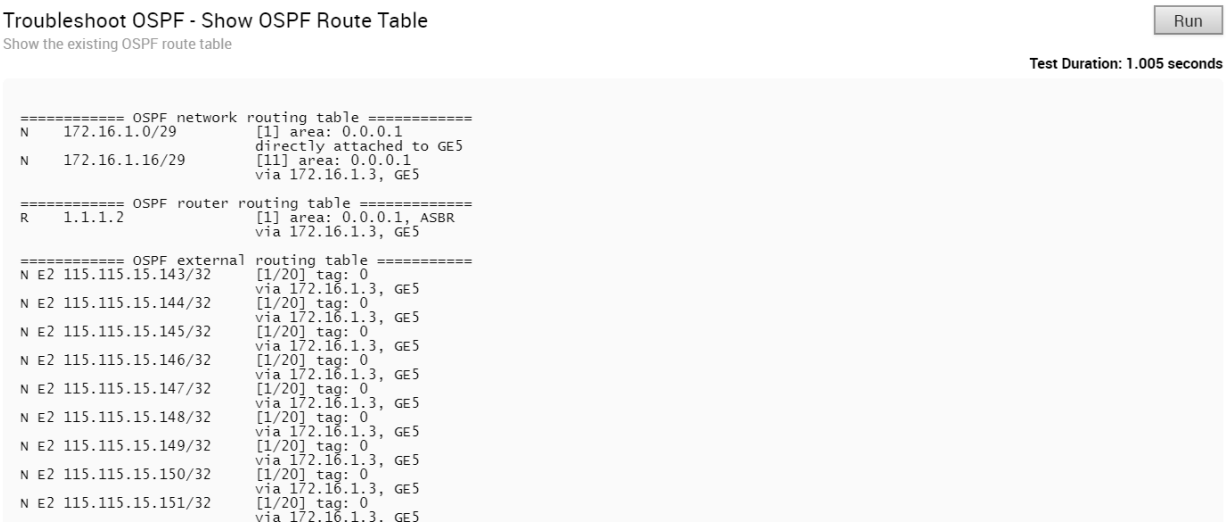


Fehlerbehebung bei OSPF – OSPF-Nachbarn anzeigen (Troubleshoot OSPF - Show OSPF Neighbors)

Führen Sie diesen Test aus, um alle OSPF-Nachbarn und zugehörige Informationen anzuzeigen.

Fehlerbehebung bei OSPF – OSPF-Routentabelle anzeigen (Troubleshoot OSPF - Show OSPF Route Table)

Führen Sie diesen Test aus, um die vorhandene OSPF-Routentabelle anzuzeigen.

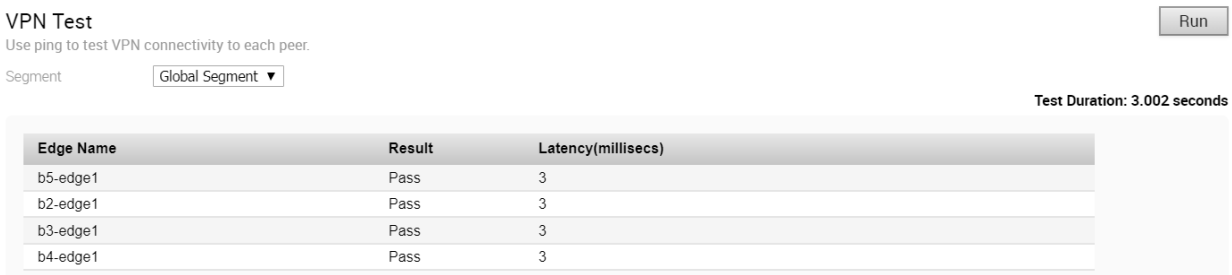


Fehlerbehebung bei OSPF – OSPF-Einstellung anzeigen (Troubleshoot OSPF - Show OSPF Setting)

Führen Sie diesen Test aus, um die OSPF-Einstellung und den Status des Nachbarn anzuzeigen.

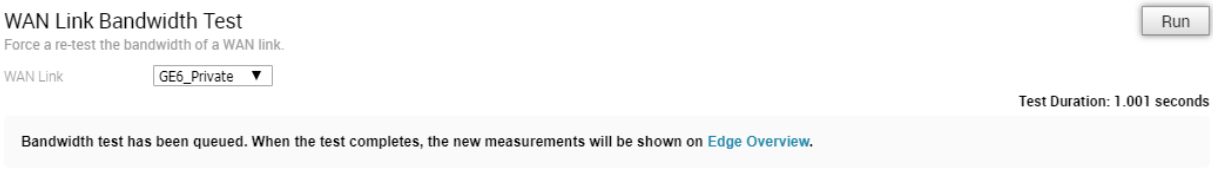
VPN-Test (VPN Test)

Verwenden Sie Ping, um die VPN-Verbindung für jeden Peer zu testen.



Bandbreitentest für WAN-Link (WAN Link Bandwidth Test)

Führen Sie den Bandbreitentest für einen angegebenen WAN-Link aus. Dieser Test hat den Vorteil, dass es in Umgebungen mit Mehrfachverknüpfungen nicht zu Störungen kommt. Nur der zu testende Link ist für den Benutzerdatenverkehr gesperrt. Das bedeutet, dass Sie den Test auf einem bestimmten Link erneut ausführen können und der bzw. die anderen Links weiterhin dem Benutzerdatenverkehr dienen.



Da der Bandbreitentest durchgeführt wird, wenn der Tunnel nach einer Zeit der Instabilität wieder eine Verbindung herstellt, gab es in der Praxis Fälle, in denen sich der Link zwar genügend für eine Tunnelkonnektivität erholt hat, aber nicht genug, um die Bandbreite des WAN-Links genau zu messen. Um diesen Szenarien Rechnung zu tragen, wird, falls der Bandbreitentest fehlschlägt oder einen deutlich reduzierten Wert misst, die letzte bekannte „fehlerfreie“ Messung verwendet und ein erneuter Link-Test für 30 Minuten nach der Einrichtung des Tunnels geplant, um eine ordnungsgemäße Messung zu gewährleisten.

Remote-Aktionen

Sie können Aktionen wie den Neustart von Diensten oder den Neustart oder die Deaktivierung eines Edge von einem Remote-Standort über das Unternehmensportal ausführen.

Die Remote-Aktionen können nur auf einem Edge ausgeführt werden, der sich im Status **Verbunden (Connected)** befindet.

1 Klicken Sie im Unternehmensportal auf **Testen und Fehlerbehebung (Test & Troubleshoot) > Remote-Aktionen (Remote Actions)**.

2 Auf der Seite **Remote-Edge-Aktionen (Remote Edge Actions)** werden alle verbundenen Edges angezeigt. Suchen Sie bei Bedarf mit dem **Filter** nach einem Edge und klicken Sie dann auf **Anwenden (Apply)**.

3 Klicken Sie auf den Link zu einem verbundenen Edge.

   Klicken Sie im Fenster **Edge-Remote-Aktionen (Edge Remote Actions)** auf die entsprechende Aktion. Die Aktion wird auf dem ausgewählten Edge ausgeführt.

4 Sie können die folgenden Aktionen ausführen:

Aktion	Beschreibung
Erkennen (Identify)	Zufälliges Blinken auf dem ausgewählten Edge zur Identifizierung des Geräts.
Dienst neu starten (Restart Service)	Startet die VMware SD-WAN-Dienste auf dem ausgewählten Edge neu.
Neustarten	Startet den ausgewählten Edge neu.
Herunterfahren (Shutdown)	Schaltet den ausgewählten Edge aus.
Deaktivieren	Setzt die Konfiguration des Geräts auf die Werkseinstellungen zurück.

Hinweis Die Ausführung der Aktionen auf dem Gerät kann bis zu einer Minute dauern.

Diagnosepakete

Mithilfe von Diagnosepaketen können Benutzer alle Konfigurationsdaten und Protokolldateien in einer konsolidierten komprimierten Datei sammeln. Die in den Diagnosepaketen verfügbaren Daten können für das Debugging verwendet werden.

Klicken Sie im Unternehmensportal auf **Testen und Fehlerbehebung (Test & Troubleshooting) > Diagnosepakete (Diagnostic Bundles)**.

Im Fenster **Diagnosepakete (Diagnostic Bundles)** können Sie die folgenden Pakete anfordern:

- **PCAP-Paket (PCAP Bundle)**: Beim Paketerfassungspaket handelt es sich um eine Sammlung von Paketdaten des Netzwerks. Operatoren, Standardadministratoren und der Kundensupport können PCAP-Pakete anfordern. Weitere Informationen finden Sie unter Anfordern der Paketerfassung.
- **Diagnosepaket (Diagnostic Bundle)**: Das Diagnosepaket ist eine Sammlung aller Konfigurationen und Protokolle eines bestimmten Edge. Nur Operatoren können Diagnosepakete anfordern. Weitere Informationen finden Sie unter Anfordern des Diagnosepakets.

Die generierten Pakete werden im Fenster **Diagnosepakete (Diagnostic Bundles)** angezeigt. Informationen zum Herunterladen der Paketdateien finden Sie unter Herunterladen eines Pakets.

Anfordern der Paketerfassung

Die Paketerfassungsfunktion wird verwendet, um Debugging-Informationen von einem Edge-Gerät zu erfassen.

Greifen Sie über **Testen und Fehlerbehebung (Test & Troubleshoot) > Paketerfassung (Packet Capture)** auf die Paketerfassung zu.

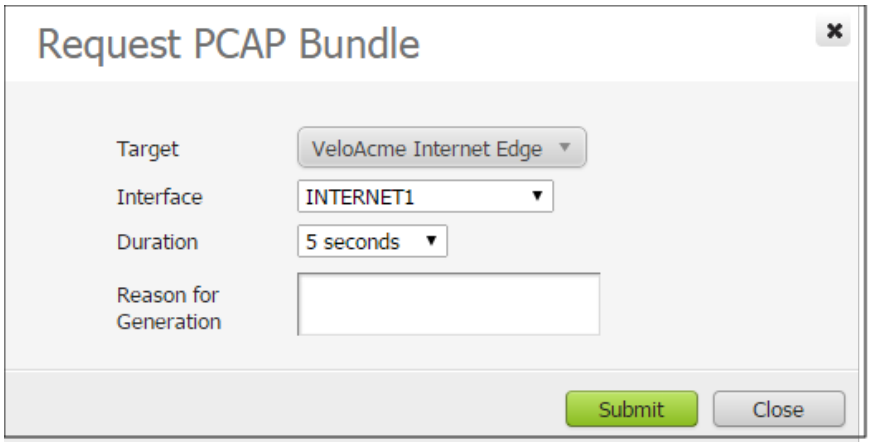
So fordern Sie eine Paketerfassung an:

1 Klicken Sie unter **Testen und Fehlerbehebung (Test & Troubleshoot)** auf **Paketerfassung (Packet Capture)**.

Der Bildschirm **Paketerfassung (Packet Capture)** wird angezeigt. Gegebenenfalls wird der Status früherer Anfragen angezeigt.

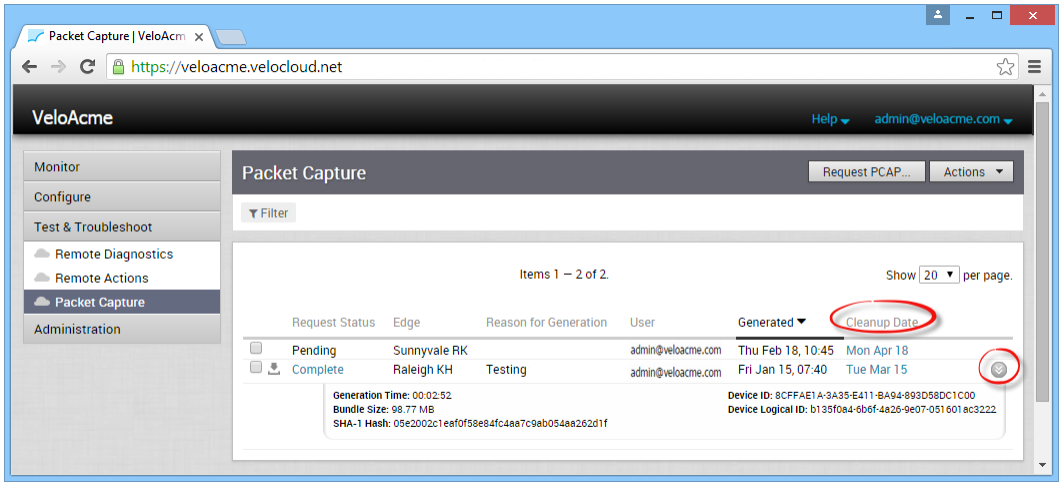
2 Klicken Sie oben rechts im Bildschirm auf **PCAP anfordern (Request PCAP)**.

3 Wählen Sie im Dialogfeld **PCAP-Paket anfordern (Request PCAP Bundle)** Ziel, Schnittstelle und Dauer aus. Geben Sie, falls erforderlich, einen Grund für die Erstellung ein.



4 Klicken Sie auf **Übermitteln (Submit)**. In der oberen rechten Ecke des Bildschirms wird eine Popup-Meldung (erfolgreiche Anforderung) angezeigt.

Der Bildschirm **Paketerfassung (Packet Capture)** wird aktualisiert und zeigt jetzt den Status der Anforderung. Aktualisieren Sie Ihren Bildschirm oder klicken Sie im Navigationsbereich auf **Paketerfassung (Packet Capture)**, um die Statusergebnisse anzuzeigen. Anschließend können Sie detaillierte Informationen (Erstellungszeit, Paketgröße usw.) anfordern, indem Sie auf den grauen Pfeil klicken, der sich neben der letzten Spalte ganz rechts befindet.



Hinweis Die Paketerfassungsdaten für einen bestimmten Edge werden an dem Datum, das in der Spalte **Bereinigungsdatum (Cleanup Date)** angezeigt wird, aus dem System gelöscht. Klicken Sie auf den Link **Bereinigungsdatum (Cleanup Date)**, um ein Datum zum Entfernen der Daten anzugeben, oder aktivieren Sie das Kontrollkästchen **Immer beibehalten (Keep Forever)**. Die Daten werden nicht gelöscht, sondern aufbewahrt, bis Sie etwas anderes angeben.

Klicken Sie auf die Schaltfläche **Aktionen (Actions)**, um das Paket herunterzuladen oder zu löschen. Weitere Informationen hierzu finden Sie in den folgenden Abschnitten.

Anfordern des Diagnosepakets

Nur Operatoren können Diagnosepakete anfordern. Wenn Sie ein Operator sind, können Sie auf die Schaltfläche **Diagnosepaket (Diagnostic Bundle)** auf der Seite **Testen und Fehlerbehebung > Diagnosepakete (Test & Troubleshooting > Diagnostic Bundles)** zugreifen.

So fordern Sie ein Diagnosepaket an:

1 Klicken Sie oben rechts auf der Seite **Diagnosepakete (Diagnostic Bundles)** auf die Schaltfläche **Diagnosepaket anfordern (Request Diagnostic Bundle)**.

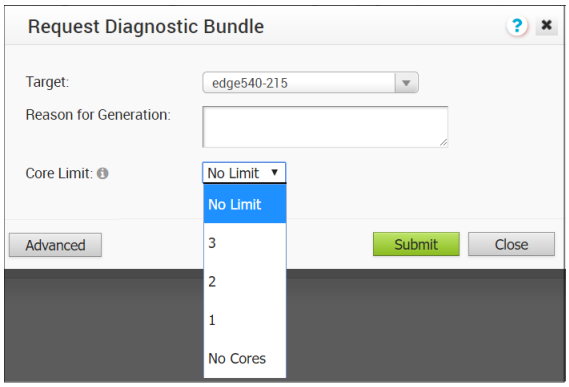
2 Gehen Sie im Dialogfeld **Diagnosepaket anfordern (Request Diagnostic Bundle)** wie folgt vor:

   a Wählen Sie im Dropdown-Menü **Ziel (Target)** den gewünschten Edge aus, von dem Sie die Daten empfangen werden.

   b Den Grund für die Anforderung können Sie bei Bedarf im Textfeld **Grund für die Erstellung (Reason for Generation)** angeben.

c Klicken Sie für eine erweiterte Anforderung auf die Schaltfläche **Erweitert (Advanced)** und wählen Sie im Dropdown-Menü **Kerngrenzwert (Core Limit)** einen Grenzwert aus. Der Kerngrenzwert wird verwendet, um die Größe des hochgeladenen Pakets zu verringern, wenn es zu Fehlern bei der Internetkonnektivität kommt.

d Klicken Sie auf die Schaltfläche „Übermitteln“ (Submit).



Das Diagnoseanforderungspaket für den ausgewählten Edge hat den Status „Ausstehend“ (Pending), wie in der Spalte „Anforderungsstatus“ (Request Status) im Fenster „Diagnosepakete“ (Diagnostic Bundles) gezeigt. Der Status ändert sich anschließend in **Abgeschlossen (Complete)**. Der Status **Abgeschlossen (Complete)** ist ein Link, über den Sie das Paket herunterladen können.

Herunterladen eines Pakets

Wenn die Anforderung abgeschlossen ist, können Sie das Paket auf eine der folgenden Arten herunterladen:

- Klicken Sie neben einer abgeschlossenen PCAP-Anforderung unter der Spalte **Anforderungsstatus (Request Status)** auf das Download-Symbol.
- Klicken Sie für Ihren ausgewählten Edge auf den Link **Abgeschlossen (Complete)** in der Spalte **Anforderungsstatus (Request Status)**.
- Aktivieren Sie das Kontrollkästchen einer oder mehrerer PCAP-Anforderungen und klicken Sie auf den nach unten weisenden Pfeil der Schaltfläche **Aktion (Action)** (obere, rechte Ecke des Bildschirms) und wählen Sie **Herunterladen (Download)** aus.

Sie können das heruntergeladene Paket an einen Mitarbeiter des VMware SD-WAN-Netzwerksupports weiterleiten.

Löschen eines Pakets

Wenn Sie eine Paketerfassung löschen möchten, wählen Sie eine oder mehrere Paketerfassungen aus der Spalte **Anforderungsstatus (Request Status)** aus und wählen Sie dann über die Schaltfläche **Aktionen (Actions)** die Option **Löschen (Delete)** aus.

Hinweis Wenn eine Anforderung zur Paketerfassung aussteht, können Sie die Anforderung vor dem Abschluss der Anforderung löschen. Aktivieren Sie das Kontrollkästchen der ausstehenden Anforderung, die Sie löschen möchten, klicken Sie auf die Schaltfläche **Aktionen (Actions)** und wählen Sie **Löschen (Delete)** aus.

Enterprise-Verwaltung

23

Mit der Option **Verwaltung (Administration)** im Enterprise-Portal können Sie die Systemeinstellungen und Authentifizierungsinformationen konfigurieren, Administratorbenutzer erstellen und Edge-Lizenzen verwalten.

Klicken Sie im Enterprise-Portal auf **Verwaltung (Administration)**, um Folgendes zu konfigurieren:

- **Systemeinstellungen (System Settings)**– Konfigurieren von Benutzerinformationen und Enterprise-Authentifizierung. Weitere Informationen finden Sie unter Systemeinstellungen.
- **Administratoren (Administrators)**– Erstellen oder Ändern von Benutzern mit verschiedenen Rollenberechtigungen. Weitere Informationen finden Sie unter Verwalten von Admin-Benutzern.
- **Edge-Lizenzierung (Edge Licensing)**– Anzeigen und Erzeugen eines Berichts der Edge-Lizenzen. Weitere Informationen finden Sie unter Edge-Lizenzierung.

Dieses Kapitel enthält die folgenden Themen:

Systemeinstellungen

Mit der Option **Systemeinstellungen (System Settings)** können Sie die Administratoreinstellungen zusammen mit den Authentifizierungsdetails konfigurieren.

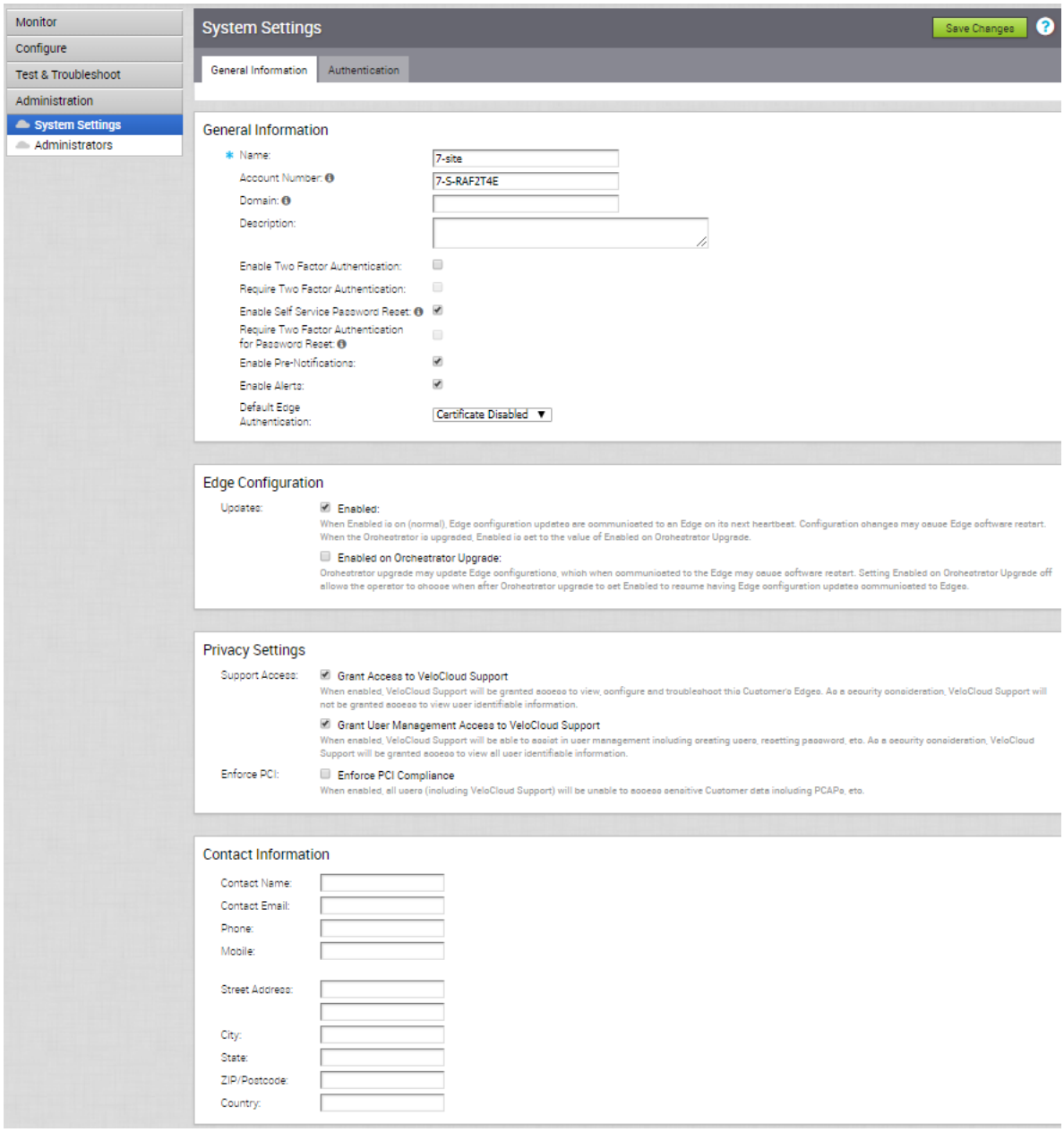
Klicken Sie im Unternehmensportal auf **Verwaltung (Administration) > Systemeinstellungen (System Settings)**, um Folgendes zu konfigurieren:

- **Allgemeine Informationen (General Information)**: Konfigurieren Sie die Benutzerdaten, aktivieren Sie die Edge-Konfigurationsaktualisierungen, konfigurieren Sie Datenschutzeinstellungen und geben Sie die Kontaktdaten ein. Weitere Informationen finden Sie unter Konfigurieren von Unternehmensinformationen.
- **Authentifizierung (Authentication)**: Konfigurieren Sie den Authentifizierungsmodus und zeigen Sie die API-Token an. Weitere Informationen finden Sie unter Konfigurieren der Unternehmensauthentifizierung.

Konfigurieren von Unternehmensinformationen

Sie können die Benutzerinformationen, Edge-Updates, Datenschutzeinstellungen und Kontaktdetails für die Benutzer mithilfe der Option **Allgemeine Informationen (General Information)** konfigurieren.

Klicken Sie im Unternehmensportal auf **Verwaltung (Administration) > Systemeinstellungen (System Settings)**. Sie können die folgenden Einstellungen auf der Registerkarte **Allgemeine Informationen (General Information)** konfigurieren.



Allgemeine Informationen (General Information)

Option	Beschreibung
Name	Der vorhandene Benutzername wird angezeigt. Bei Bedarf können Sie den Namen ändern.
Kontonummer (Account Number)	Die vorhandene Kontonummer wird angezeigt. Falls erforderlich, können Sie die Nummer ändern.
Domäne (Domain)	Der vorhandene Domänenname wird angezeigt. Bei Bedarf können Sie die Domäne ändern.
Beschreibung (Description)	Geben Sie eine Beschreibung für den Kunden ein.
Zwei-Faktor-Authentifizierung aktivieren (Enable Two Factor Authentication)	Aktivieren Sie das Kontrollkästchen, um die Zwei-Faktor-Authentifizierung mit SMS für Operatoren, MSP und Unternehmen zu aktivieren. Sie können die Authentifizierung auf der Kunden-/MSP-Ebene oder auf der Operator-Ebene aktivieren. Stellen Sie sicher, dass Sie allen Admin-Benutzern gültige Mobilnummern bereitgestellt haben, bevor Sie die Zwei-Faktor-Authentifizierung aktivieren. Sie können die Mobilnummern eingeben, indem Sie die Benutzer im Bildschirm **Verwaltung (Administration) > Administratoren (Administrators)** auswählen. Weitere Informationen finden Sie auch unter Verwalten von Admin-Benutzern.
Zwei-Faktor-Authentifizierung anfordern (Require Two Factor Authentication)	Aktivieren Sie das Kontrollkästchen, um die Benutzeranmeldung mit Zwei-Faktor-Authentifizierung festzulegen. Wenn Sie nach dem Aktivieren der Zwei-Faktor-Authentifizierung versuchen, sich mit Ihren Benutzeranmeldedaten anzumelden, müssen Sie auch die sechsstellige PIN eingeben, die Sie als SMS auf Ihrem Mobiltelefon erhalten.
Self-Service-Kennwortzurücksetzung aktivieren (Enable Self Service Password Reset)	Standardmäßig ist diese Option ausgewählt, sodass Sie Ihr Kennwort auf der Orchestrator-Anmeldeseite zurücksetzen können. Wenn Sie versuchen, Ihr Kennwort auf der Anmeldeseite zurückzusetzen, werden Sie aufgefordert, einen Benutzernamen einzugeben. Stellen Sie sicher, dass Sie eine gültige E-Mail-Adresse als Benutzername eingeben. Sobald Sie den Benutzernamen gesendet haben, erhalten Sie eine E-Mail mit einem Link zum Zurücksetzen des Kennworts. Klicken Sie auf den Link, um ein neues Kennwort einzurichten.

Option	Beschreibung
Zwei-Faktor-Authentifizierung für Kennwortzurücksetzung anfordern (Require Two Factor Authentication for Password Reset)	Wählen Sie diese Option aus, um die Zwei-Faktor-Authentifizierung zum Zurücksetzen Ihres Kennworts zu aktivieren. Sie können dieses Kontrollkästchen nur dann aktivieren, wenn die Option **Zwei-Faktor-Authentifizierung aktivieren (Enable Two Factor Authentication)** bereits ausgewählt ist. Wenn diese Option aktiviert ist und Sie versuchen, Ihr Kennwort auf der Orchestrator-Anmeldeseite zurückzusetzen, werden Sie zu einer Authentifizierungsseite umgeleitet. Auf der Seite „Authentifizierung (Authentication)“ werden Sie aufgefordert, den einmaligen Code einzugeben, den Sie als SMS auf Ihrem Mobiltelefon erhalten. Nach dem Validieren des Codes werden Sie zur Seite „Kennwort (Password)“ weitergeleitet, um ein neues Kennwort einzurichten.
Vorabbenachrichtigungen aktivieren (Enable Pre-Notifications)	Aktivieren Sie das Kontrollkästchen, um Vorabwarnungen zu aktivieren.
Warnungen aktivieren (Enable Alerts)	Aktivieren Sie das Kontrollkästchen, um die Warnungen zu aktivieren. Sie können die Warnungstypen mithilfe der Option Kapitel 21 Konfigurieren von Warnungen konfigurieren.
Edge-Standardauthentifizierung (Default Edge Authentication)	Wählen Sie die Standardoption zum Authentifizieren der mit dem Kunden verknüpften Edges in der Dropdown-Liste aus.

Edge-Konfiguration (Edge Configuration)

Wählen Sie die folgenden Optionen aus, um die Updates zu den Edge-Konfigurationen an einen Edge zu übermitteln:

- **Aktiviert (Enabled)**: Wählen Sie diese Option aus, um die Konfigurations-Updates beim nächsten Taktsignal an einen Edge zu übermitteln. Die Änderungen an der Konfiguration können die Software im entsprechenden Edge neu starten. Diese Option ist standardmäßig ausgewählt.
- **Aktivierung bei Orchestrator-Update (Enabled on Orchestrator Upgrade)**: Wählen Sie diese Option, um die Updates in den Konfigurationen an die Edges zu übermitteln, wenn die Orchestrator-Instanz aktualisiert wird. Dadurch kann die Software auf den entsprechenden Edges neu gestartet werden.

Datenschutzeinstellungen (Privacy Settings)

- **Supportzugriff (Support Access)**: Wählen Sie die folgenden Optionen, um dem Supportteam Zugriff zu gewähren.
  - **Zugriff auf VeloCloud-Support gewähren (Grant Access to VeloCloud Support)**: Wählen Sie diese Option aus, um dem VMware SD-WAN-Support Zugriff zu gewähren, um die mit dem Kunden verbundenen Edges anzuzeigen, zu konfigurieren und Fehler zu beheben. Aus Sicherheitsgründen kann der Support nicht auf die identifizierbaren Informationen des Benutzers zugreifen oder diese anzeigen.
  - **Benutzerverwaltungszugriff für VeloCloud-Support gewähren (Grant User Management Access to VeloCloud Support)**: Wählen Sie diese Option aus, um den VMware SD-WAN-Support zur Unterstützung der Benutzerverwaltung zu aktivieren. Die Benutzerverwaltung umfasst Optionen zum Erstellen von Benutzern, zum Zurücksetzen des Kennworts und zum Konfigurieren anderer Einstellungen. In diesem Fall hat der Support Zugriff auf identifizierbare Informationen des Benutzers.
- **PCI erzwingen (Enforce PCI)**: Wählen Sie diese Option aus, um die PCI-Übereinstimmung auf der Orchestrator-Instanz zu erzwingen. Sobald Sie diese Option aktiviert haben, blockiert die Orchestrator-Instanz den Zugriff auf vertrauliche Kundendaten, einschließlich PCAPs, für alle Benutzer.

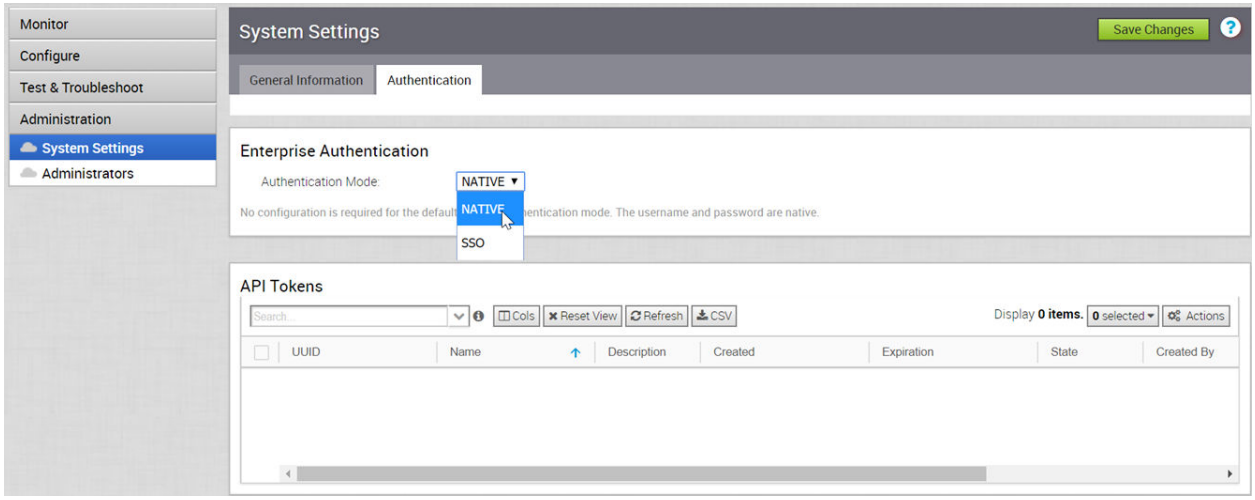
Kontaktinformationen (Contact Information)

Die vorhandenen Kontaktdetails werden in diesem Abschnitt angezeigt. Bei Bedarf können Sie die Details ändern.

Konfigurieren der Unternehmensauthentifizierung

Auf der Registerkarte **Authentifizierung (Authentication)** können Sie den Authentifizierungsmodus für die Unternehmen einrichten und die vorhandenen API-Token anzeigen.

Klicken Sie im Unternehmensportal auf **Verwaltung (Administration) > Systemeinstellungen (System Settings) > Authentifizierung (Authentication)**, um folgende Einstellungen zu konfigurieren:



Enterprise-Authentifizierung (Enterprise Authentication)

Wählen Sie eine der folgenden Optionen für den **Authentifizierungsmodus (Authentication Mode)**.

- **NATIV (NATIVE)**: Dies ist der Standardauthentifizierungsmodus, und Sie können sich mit dem nativen Benutzernamen und Kennwort beim Unternehmen anmelden. Für diesen Modus ist keine Konfiguration erforderlich.
- **SSO**: Single Sign-On (SSO) ist ein Sitzungs- und Benutzerauthentifizierungsdienst, der es den Benutzern ermöglicht, sich mit einem Satz von Anmeldedaten beim Unternehmen anzumelden, um auf mehrere Anwendungen zuzugreifen. Weitere Informationen finden Sie unter Übersicht über Single Sign-On und Konfigurieren von Single Sign-On für Unternehmensbenutzer.

API-Token (API Tokens)

Sie können auf die Orchestrator-APIs mit tokenbasierter Authentifizierung zugreifen, unabhängig vom Authentifizierungsmodus. Sie können die vorhandenen API-Token in diesem Abschnitt anzeigen.

Der Operator-Superuser oder der mit einem API-Token verbundene Benutzer kann das Token widerrufen. Wählen Sie das Token aus und klicken Sie auf **Aktionen (Actions) > Widerrufen (Revoke)**. Weitere Informationen zum Erstellen und Download der API-Token finden Sie unter API-Token.

Übersicht über Single Sign-On

SD-WAN Orchestrator unterstützt einen neuen Typ der Benutzerauthentifizierung namens Single Sign-On (SSO) für alle Orchestrator-Benutzertypen: Operator, Partner und Enterprise.

Single Sign-On (SSO) ist ein Sitzungs- und Benutzerauthentifizierungsdienst, der es SD-WAN Orchestrator-Benutzern ermöglicht, sich bei SD-WAN Orchestrator mit einem Satz von Anmeldedaten anzumelden, um auf mehrere Anwendungen zuzugreifen. Durch die Vernetzung des SSO-Diensts mit SD-WAN Orchestrator wird die Sicherheit der Benutzerauthentifizierung für SD-WAN Orchestrator-Benutzer verwendet, und SD-WAN Orchestrator erhält die Möglichkeit, Benutzer von anderen OpenID Connect (OIDC)-basierten Identitätsanbietern (IDPs) zu authentifizieren. Die folgenden IDPs werden zurzeit unterstützt:

- Okta
- OneLogin
- PingIdentity
- AzureAD
- VMwareCSP

Konfigurieren von Single Sign-On für Unternehmensbenutzer

Führen Sie die Schritte in diesem Verfahren aus, um Single Sign-On (SSO)-Authentifizierung für Unternehmensbenutzer einzurichten.

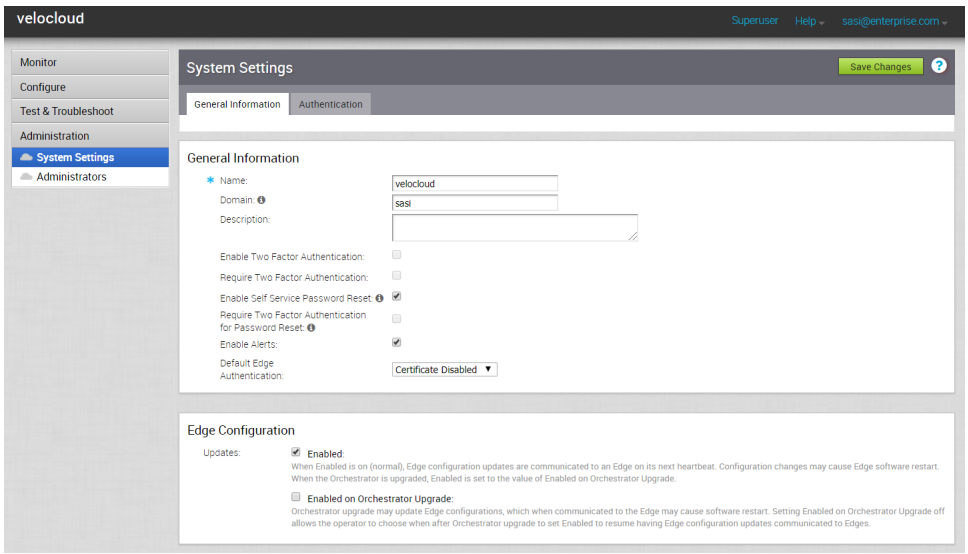
Voraussetzungen

- Stellen Sie sicher, dass Sie über die Berechtigung für Unternehmens-Superuser verfügen.
- Stellen Sie vor dem Einrichten der SSO-Authentifizierung sicher, dass Sie Rollen, Benutzer und OpenID Connect (OIDC)-Anwendung für SD-WAN Orchestrator auf der Website Ihres bevorzugten Identitätsanbieters eingerichtet haben. Weitere Informationen finden Sie unter Konfigurieren eines IDP für Single Sign-On.

Verfahren

1. Melden Sie sich bei einer SD-WAN Orchestrator-Anwendung als Unternehmens-Superuser mit Ihren Anmeldedaten an.
2. Klicken Sie auf **Verwaltung (Administration)** > **Systemeinstellungen (System Settings)**.

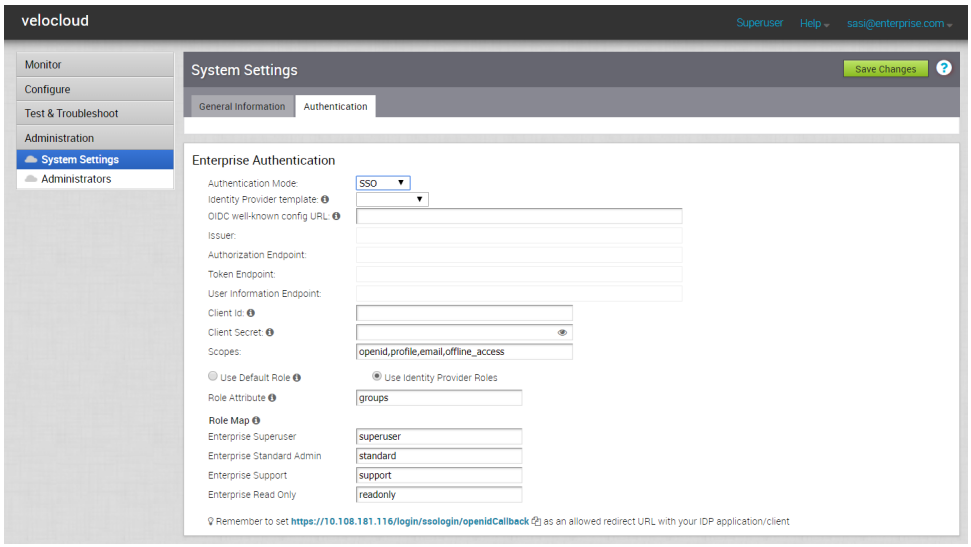
   Der Bildschirm **Systemeinstellungen (System Settings)** wird angezeigt.



3 Klicken Sie auf die Registerkarte **Allgemeine Informationen (General Information)** und geben Sie im Textfeld **Domäne (Domain)** den Domänennamen für Ihr Unternehmen ein, sofern er noch nicht festgelegt ist.

Hinweis Um die SSO-Authentifizierung für die SD-WAN Orchestrator-Instanz zu aktivieren, müssen Sie den Domänennamen für Ihr Unternehmen einrichten.

4 Klicken Sie auf die Registerkarte **Authentifizierung (Authentication)** und wählen Sie im Dropdown-Menü **Authentifizierungsmodus (Authentication Mode)** den Eintrag **SSO** aus.



5 Wählen Sie im Dropdown-Menü **Identitätsanbietervorlage (Identity Provider template)** den bevorzugten Identitätsanbieter (Identity Provider, IDP) aus, den Sie für Single Sign-On konfiguriert haben.

Hinweis Wenn Sie VMwareCSP als bevorzugten Identitätsanbieter auswählen, stellen Sie sicher, dass Sie Ihre Organisations-ID im folgenden Format angeben: */csp/gateway/am/api/orgs/<full organization ID>*.

Wenn Sie sich bei der VMware CSP-Konsole anmelden, können Sie durch Klicken auf Ihren Benutzernamen die ID der Organisation anzeigen, bei der Sie angemeldet sind. Eine verkürzte Version der ID wird unter dem Organisationsnamen angezeigt. Klicken Sie auf die ID, um die vollständige Organisations-ID anzuzeigen.

Sie können Ihre eigenen IDPs auch manuell konfigurieren, indem Sie **Sonstige (Others)** im Dropdown-Menü **Identitätsanbietervorlage (Identity Provider template)** auswählen.

6 Geben Sie im Textfeld **Bekannte URL für die Konfiguration von OIDC (OIDC well-known config URL)** die OIDC-Konfigurations-URL (OpenID Connect) für Ihren IDP ein. Beispielsweise lautet das URL-Format für Okta: https://{oauth-provider-url}/.well-known/openid-configuration.

7 In der SD-WAN Orchestrator-Anwendung werden Endpoint-Details, wie z. B. Aussteller, Autorisierungs-Endpoint, Token-Endpoint und Benutzerinformations-Endpoint, für Ihren IDP automatisch befüllt.

8 Geben Sie im Textfeld **Client-ID (Client ID)** die vom IDP bereitgestellte Client-ID ein.

9 Geben Sie im Textfeld **Geheimer Clientschlüssel (Client Secret)** den vom IDP bereitgestellten Code des geheimen Client-Schlüssels ein, der vom Client zum Austauschen eines Autorisierungscodes für ein Token verwendet wird.

10 Wählen Sie eine der folgenden Optionen aus, um die Rolle des Benutzers in SD-WAN Orchestrator zu ermitteln:

- **Standardrolle verwenden (Use Default Role)** – Ermöglicht Benutzern die Konfiguration einer statischen Rolle als Standardwert mithilfe des Textfelds **Standardrolle (Default Role)**, das bei Auswahl dieser Option angezeigt wird. Zu den unterstützten Rollen gehören: Unternehmens-Superuser (Enterprise Superuser), Unternehmens-Standardadministrator (Enterprise Standard Admin), Unternehmenssupport (Enterprise Support) und Unternehmensbenutzer mit Lesezugriff (Enterprise Read Only).

Hinweis Wenn bei der Einrichtung einer SSO-Konfiguration die Option **Standardrolle verwenden (Use Default Role)** ausgewählt wird und eine Standardbenutzerrolle definiert wird, wird allen SSO-Benutzern die angegebene Standardrolle zugewiesen. Statt einen Benutzer mit der Standardrolle zuzuweisen, kann ein Standardadministrator-Superuser oder ein Standardadministrator einen bestimmten Benutzer im Vorhinein als nicht nativen Benutzer registrieren und eine bestimmte Benutzerrolle definieren, indem er auf die Registerkarte **Verwaltung (Administration) > Administratoren (Administrators)** im Unternehmensportal klickt. Schritte zum Konfigurieren eines neuen Administratorbenutzers finden Sie unter Erstellen von neuen Admin-Benutzern.

- **Identitätsanbieterrollen verwenden (Use Identity Provider Roles)** – Verwendet die in einem IDP eingerichteten Rollen.

11 Geben Sie bei Auswahl der Option **Identitätsanbieterrollen verwenden (Use Identity Provider Roles)** im Textfeld **Rollenattribut (Role Attribute)** den Namen des im IDP festgelegten Attributs ein, um Rollen zurückzugeben.

12 Ordnen Sie im Bereich **Rollenzuordnung (Role Map)** jeder SD-WAN Orchestrator-Rolle die vom IDP bereitgestellten Rollen zu und trennen Sie diese durch Kommas.

Rollen in VMware CSP weisen folgendes Format auf: *external/<service definition uuid>/ <service role name mentioned during service template creation>.*

13 Aktualisieren Sie die zulässigen Weiterleitungs-URLs auf der Website des OIDC-Anbieters mit der SD-WAN Orchestrator-URL (https://<vco>/login/ssologin/openidCallback).

14 Klicken Sie auf **Änderungen speichern (Save Changes)**, um die SSO-Konfiguration zu speichern.

15 Klicken Sie auf **Konfiguration testen (Test Configuration)**, um die eingegebene OIDC-Konfiguration (OpenID Connect) zu validieren.

Der Benutzer wird an die Website des IDP weitergeleitet und kann dort die Anmeldedaten eingeben. Nach der IDP-Verifizierung und erfolgreichen Weiterleitung zum SD-WAN Orchestrator-Test-Callback wird eine erfolgreiche Validierungsmeldung angezeigt.

Ergebnisse

Die Einrichtung der SSO-Authentifizierung ist abgeschlossen.

Nächste Schritte

Kapitel 5 Anmelden bei VMware SD-WAN Orchestrator mithilfe von SSO für Unternehmensbenutzer.

Konfigurieren eines IDP für Single Sign-On

Um Single Sign-On (SSO) für SD-WAN Orchestrator zu aktivieren, müssen Sie einen Identitätspartner (IDP) mit Details zu SD-WAN Orchestrator konfigurieren. Zurzeit werden die folgenden IDPs unterstützt: Okta, OneLogin, PingIdentity, AzureAD und VMware CSP.

Schrittweise Anleitungen zum Konfigurieren einer OpenID Connect (OIDC)-Anwendung für SD-WAN Orchestrator in verschiedenen IDPs finden Sie unter:

- Konfigurieren von Okta für Single Sign-On
- Konfigurieren von OneLogin für Single Sign-On
- Konfigurieren von PingIdentity für Single Sign-On
- Konfigurieren von Azure Active Directory für Single Sign-On
- Konfigurieren von VMware CSP für Single Sign-On

Konfigurieren von Okta für Single Sign-On

Um OpenID Connect (OIDC)-basiertes Single Sign-On (SSO) von Okta zu unterstützen, müssen Sie zunächst eine Anwendung in Okta einrichten. Um eine OIDC-basierte Anwendung in Okta für SSO einzurichten, führen Sie die Schritte dieses Verfahrens aus.

Voraussetzungen

Stellen Sie sicher, dass Sie über ein Okta-Konto verfügen.

Verfahren

1 Melden Sie sich bei Ihrem Okta-Konto als Admin-Benutzer an.

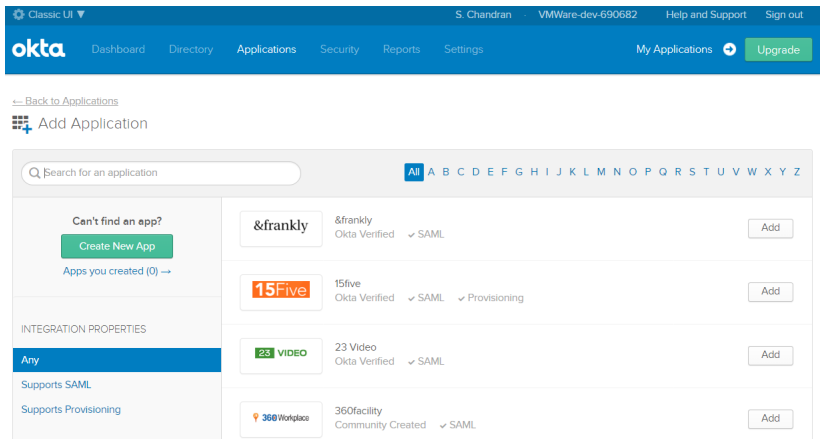
Der **Okta**-Startbildschirm wird angezeigt.

Hinweis Wenn Sie sich in der Ansicht „Entwicklerkonsole (Developer Console)“ befinden, müssen Sie zur Ansicht der klassischen Benutzeroberfläche wechseln, indem Sie in der Dropdown-Liste **Klassische Benutzeroberfläche (Classic UI)** die Option **Entwicklerkonsole (Developer Console)** auswählen.

2 So erstellen Sie eine neue Anwendung:

a Klicken Sie in der oberen Navigationsleiste auf **Anwendungen (Applications)** > **Anwendung hinzufügen (Add Application)**.

Der Bildschirm **Anwendung hinzufügen (Add Application)** wird angezeigt.



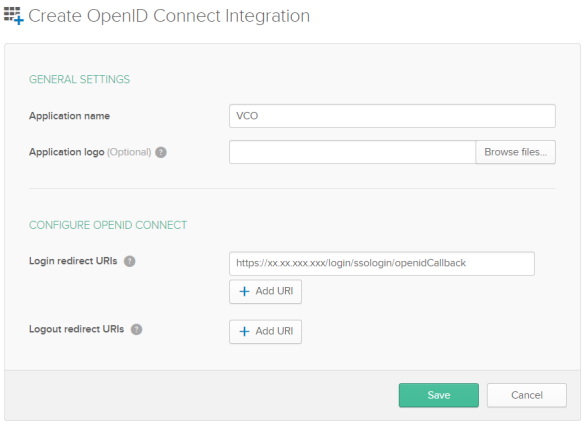
b Klicken Sie auf **Neue App erstellen (Create New App)**.

Das Dialogfeld **Neue Anwendungsintegration erstellen (Create a New Application Integration)** wird angezeigt.

c Wählen Sie im Dropdown-Menü **Plattform (Platform)** die Option **Web** aus.

d Wählen Sie **OpenID Connect** als Anmeldemethode aus und klicken Sie auf **Erstellen (Create)**.

Der Bildschirm **OpenID Connect-Integration erstellen (Create OpenID Connect Integration)** wird angezeigt.



e Geben Sie im Bereich **Allgemeine Informationen (General Settings)** im Textfeld **Anwendungsname (Application name)** den Dateinamen für Ihre Anwendung ein.

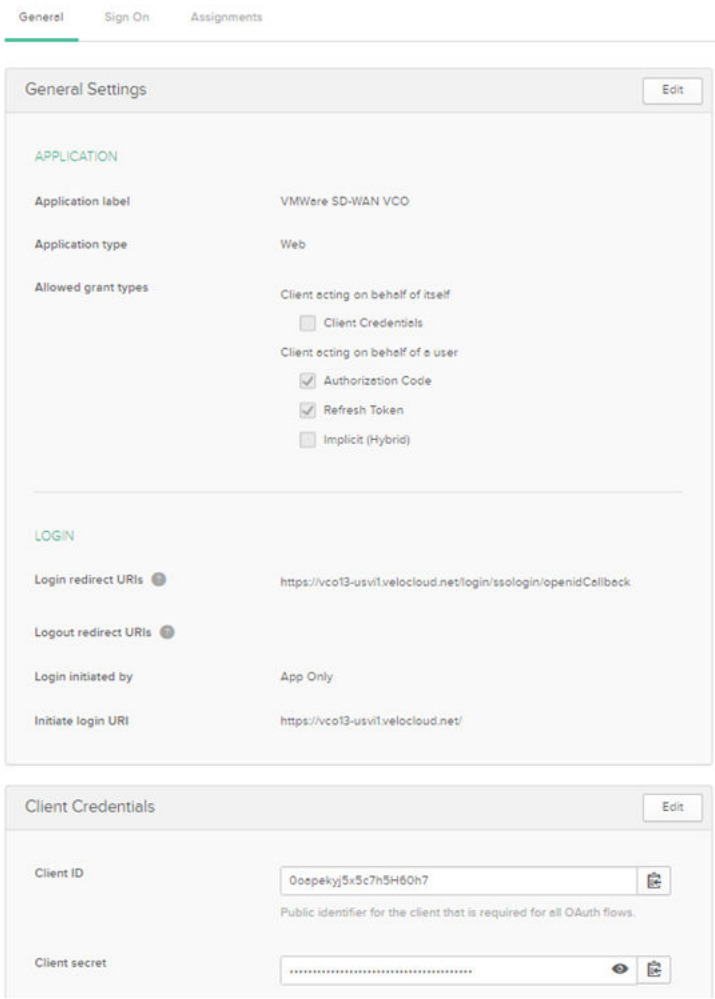
f Geben Sie im Feld **OPENID CONNECT KONFIGURIEREN (CONFIGURE OPENID CONNECT)** im Textfeld **Anmeldeumleitungs-URIs (Login redirect URIs)** die Umleitungs-URL ein, die Ihre SD-WAN Orchestrator-Anwendung als Callback-Endpoint verwendet.

In der SD-WAN Orchestrator-Anwendung finden Sie im unteren Bereich des Bildschirms **Authentifizierung konfigurieren (Configure Authentication)** den Link für die Umleitungs-URL. Idealerweise liegt die SD-WAN Orchestrator-Umleitungs-URL in diesem Format vor: https://<Orchestrator-URL>/login/ssologin/openidCallback.

g Klicken Sie auf **Speichern (Save)**. Die neu erstellte Anwendungsseite wird angezeigt.

h Klicken Sie auf der Registerkarte **Allgemein (General)** auf **Bearbeiten (Edit)** und wählen Sie **Token aktualisieren (Refresh Token)** als zulässige Gewährungstypen aus und klicken Sie auf **Speichern (Save)**.

Notieren Sie die Clientanmeldedaten (Client-ID und geheimer Clientschlüssel), die während der SSO-Konfiguration in SD-WAN Orchestrator verwendet werden sollen.



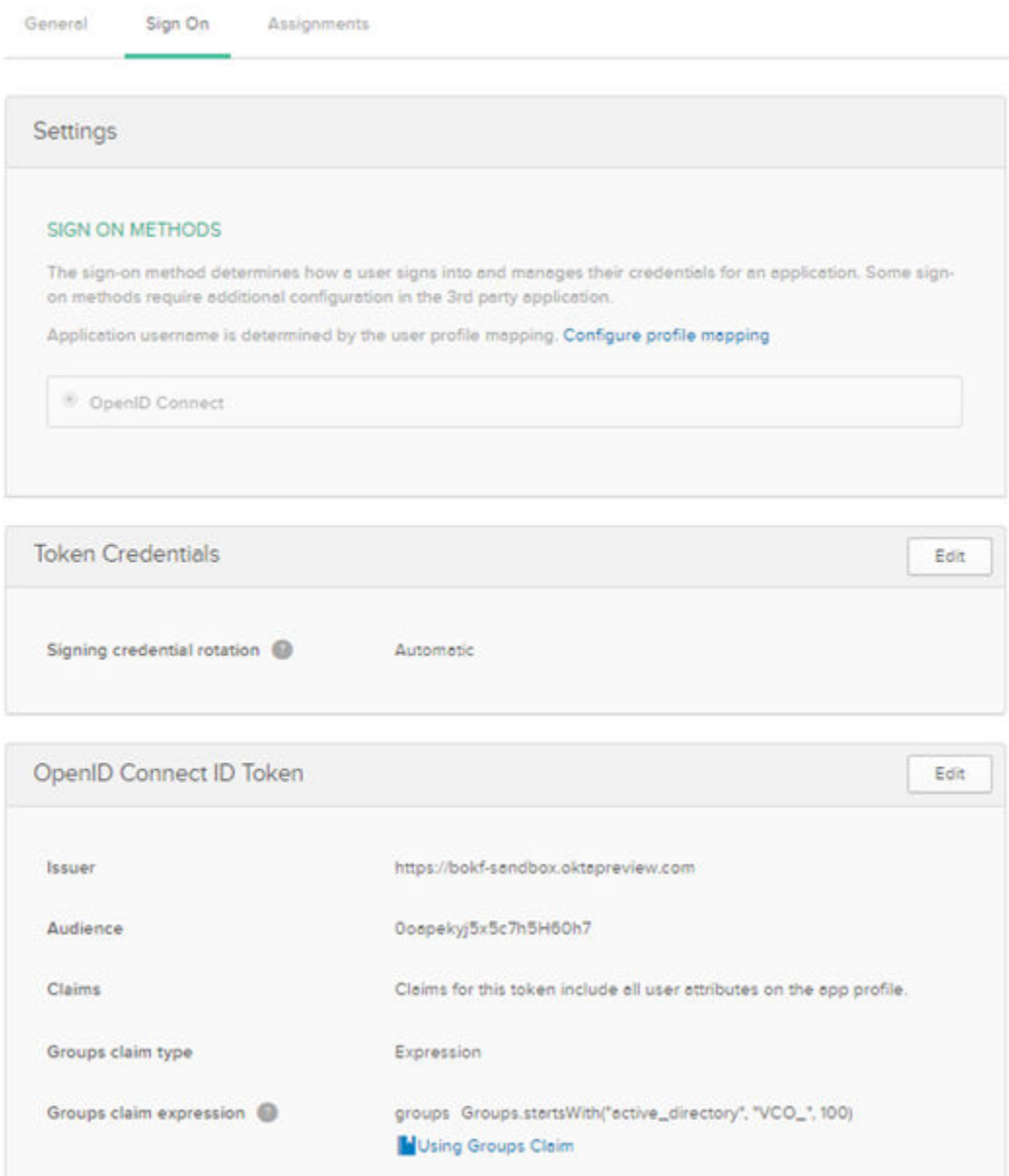
i Klicken Sie auf die Registerkarte **Anmelden (Sign On)** und klicken Sie unter dem Bereich **OpenID Connect-ID (OpenID Connect ID)** auf **Bearbeiten (Edit)**.

j Wählen Sie im Dropdown-Menü **Gruppenbeanspruchungstyp (Groups claim type)** die Option **Ausdruck (Expression)** aus. Standardmäßig ist der Gruppenbeanspruchungstyp auf **Filter** festgelegt.

k Geben Sie im Textfeld **Gruppenbeanspruchungsausdruck (Groups claim expression)** den Beanspruchungsnamen ein, der im Token verwendet wird, und geben Sie eine Okta-Eingabeausdrucksanweisung ein, die das Token auswertet.

l Klicken Sie auf **Speichern (Save)**.

Die Anwendung ist in IDP eingerichtet. Sie können Ihrer SD-WAN Orchestrator-Anwendung Benutzergruppen und Benutzer zuweisen.



3 So weisen Sie Ihrer SD-WAN Orchestrator-Anwendung Gruppen und Benutzer zu:

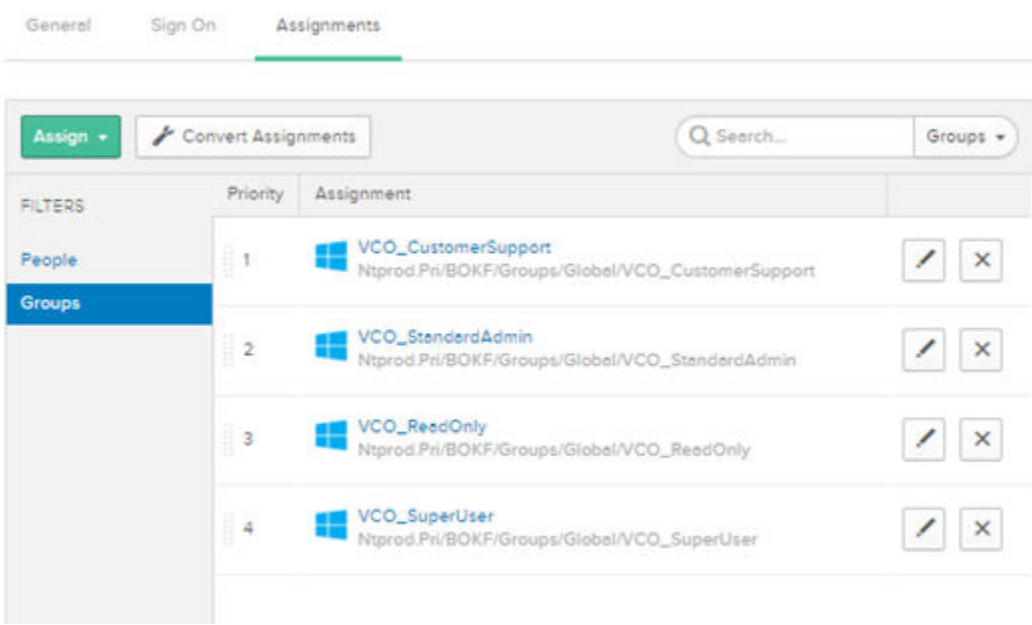
a Navigieren Sie zu **Anwendung (Application)** > **Anwendungen (Applications)** und klicken Sie auf den SD-WAN Orchestrator-Anwendungslink.

b Wählen Sie auf der Registerkarte **Zuweisungen (Assignments)** im Dropdown-Menü **Zuweisen (Assign)** die Option **Zu Gruppen zuweisen (Assign to Groups)** oder **Zu Personen zuweisen (Assign to People)** aus.

Das Dialogfeld **<Anwendungsname> zu Gruppen zuweisen (Assign <Application Name> to Groups)** oder **<Anwendungsname> zu Personen zuweisen (Assign <Application Name> to People)** wird angezeigt.

c Klicken Sie neben den verfügbaren Benutzergruppen oder Benutzern, denen Sie die SD-WAN Orchestrator-Anwendung zuweisen möchten, auf **Zuweisen (Assign)** und dann auf **Fertig (Done)**.

Die Benutzer oder Benutzergruppen, die der SD-WAN Orchestrator-Anwendung zugewiesen sind, werden angezeigt.



Ergebnisse

Sie haben die Einrichtung einer OIDC-basierten Anwendung in Okta für SSO abgeschlossen.

Nächste Schritte

Konfigurieren Sie Single Sign-On in SD-WAN Orchestrator.

Erstellen einer neuen Benutzergruppe in Okta

Um eine neue Benutzergruppe zu erstellen, führen Sie die Schritte in diesem Verfahren aus.

Verfahren

1 Klicken Sie auf **Verzeichnis (Directory)** > **Gruppen (Groups)**.

2 Klicken Sie auf **Gruppe hinzufügen (Add Group)**.

Das Dialogfeld **Gruppe hinzufügen (Add Group)** wird angezeigt.

3 Geben Sie den Gruppennamen und die Beschreibung für die Gruppe ein und klicken Sie auf **Speichern (Save)**.

Erstellen eines neuen Benutzers in Okta

Um einen neuen Benutzer hinzuzufügen, führen Sie die Schritte in diesem Verfahren aus.

Verfahren

1 Klicken Sie auf **Verzeichnis (Directory)** > **Personen (People)**.

2 Klicken Sie auf **Person hinzufügen (Add Person)**.

Das Dialogfeld **Person hinzufügen (Add Person)** wird angezeigt.

3 Geben Sie alle obligatorischen Details ein, wie z. B. Vorname, Nachname und E-Mail-ID des Benutzers.

4 Wenn Sie das Kennwort festlegen möchten, wählen Sie im Dropdown-Menü **Kennwort (Password)** die Option **Vom Benutzer festgelegt (Set by user)** aus und aktivieren Sie **Benutzeraktivierungs-E-Mail jetzt senden (Send user activation email now)**.

5 Klicken Sie auf **Speichern (Save)**.

Eine E-Mail mit einem Aktivierungslink wird an Ihre E-Mail-ID gesendet. Klicken Sie auf den Link in der E-Mail, um Ihr Okta-Benutzerkonto zu aktivieren.

Konfigurieren von OneLogin für Single Sign-On

Um eine OpenID Connect (OIDC)-basierte Anwendung in OneLogin für Single Sign-On (SSO) einzurichten, führen Sie die Schritte in diesem Verfahren aus.

Voraussetzungen

Stellen Sie sicher, dass Sie über ein OneLogin-Konto für die Anmeldung verfügen.

Verfahren

1 Melden Sie sich bei Ihrem OneLogin-Konto als Admin-Benutzer an.

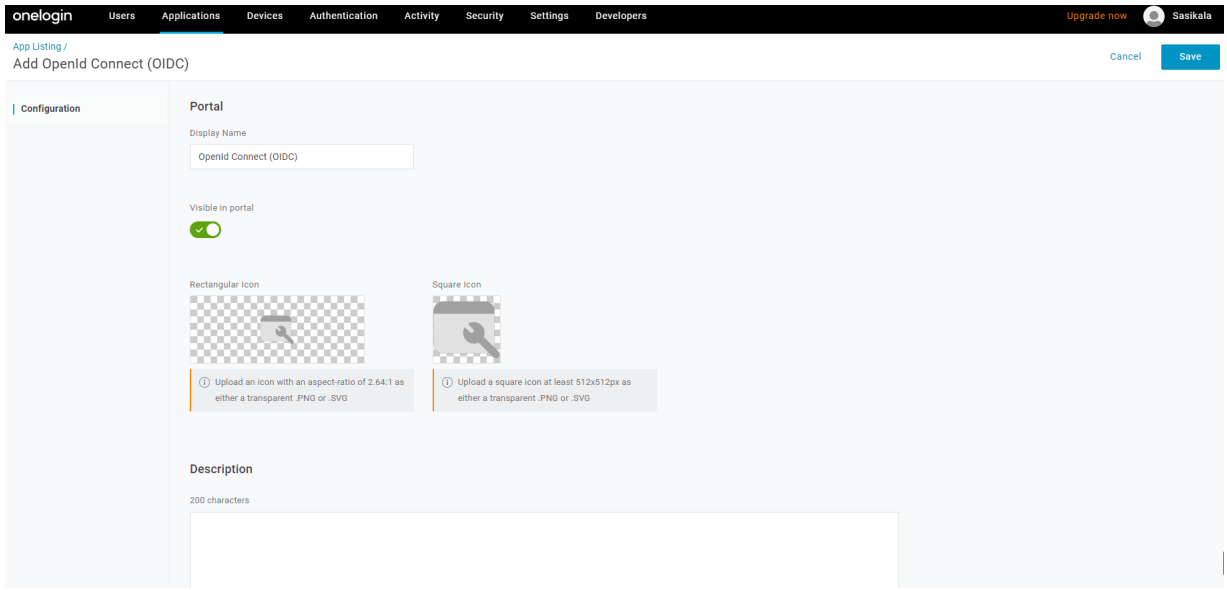
Der **OneLogin**-Startbildschirm wird angezeigt.

2 So erstellen Sie eine neue Anwendung:

a Klicken Sie in der oberen Navigationsleiste auf **Apps** > **Apps hinzufügen (Add Apps)**.

b Suchen Sie im Textfeld **Anwendungen suchen (Find Applications)** nach „OpenID Connect“ oder „oidc“ und wählen Sie dann die **OpenID Connect (OIDC)**-App aus.

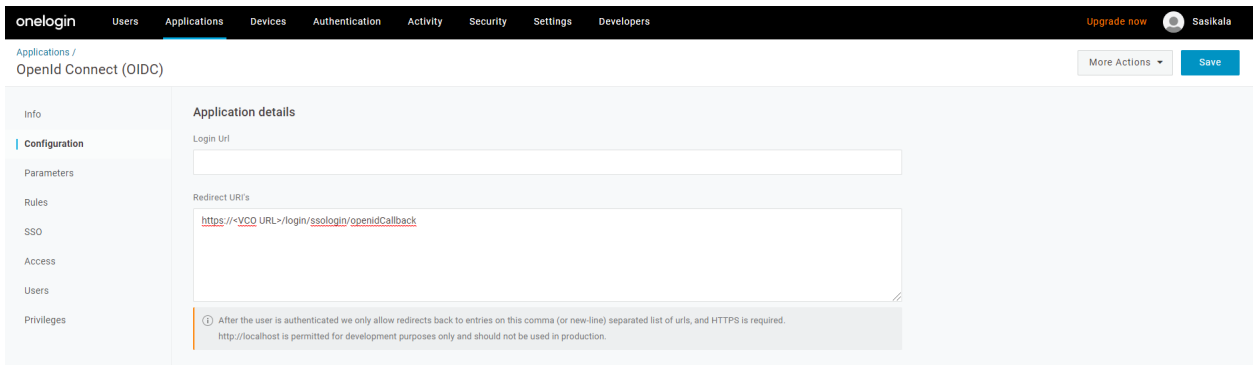
Der Bildschirm **OpenId Connect (OIDC) hinzufügen (Add OpenId Connect (OIDC))** wird angezeigt.



c Geben Sie im Textfeld **Anzeigename (Display Name)** den Namen für Ihre Anwendung ein und klicken Sie auf **Speichern (Save)**.

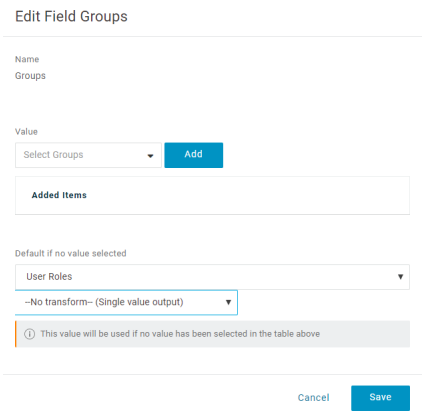
d Geben Sie auf der Registerkarte **Konfiguration (Configuration)** den Umleitungs-URI ein, den SD-WAN Orchestrator als Callback-Endpoint verwendet, und klicken Sie auf **Speichern (Save)**.

In der SD-WAN Orchestrator-Anwendung finden Sie unten im Bildschirm **Authentifizierung (Authentication)** den Link zum Umleiten der URL. Idealerweise liegt die SD-WAN Orchestrator-Umleitungs-URL in diesem Format vor: https://<Orchestrator-URL>/login/ssologin/openidCallback.



e Doppelklicken Sie auf der Registerkarte **Parameter (Parameters)** unter **OpenID Connect (OIDC)** auf **Gruppen (Groups)**.

Das Popup-Fenster **Feldgruppen bearbeiten (Edit Field Groups)** wird angezeigt.

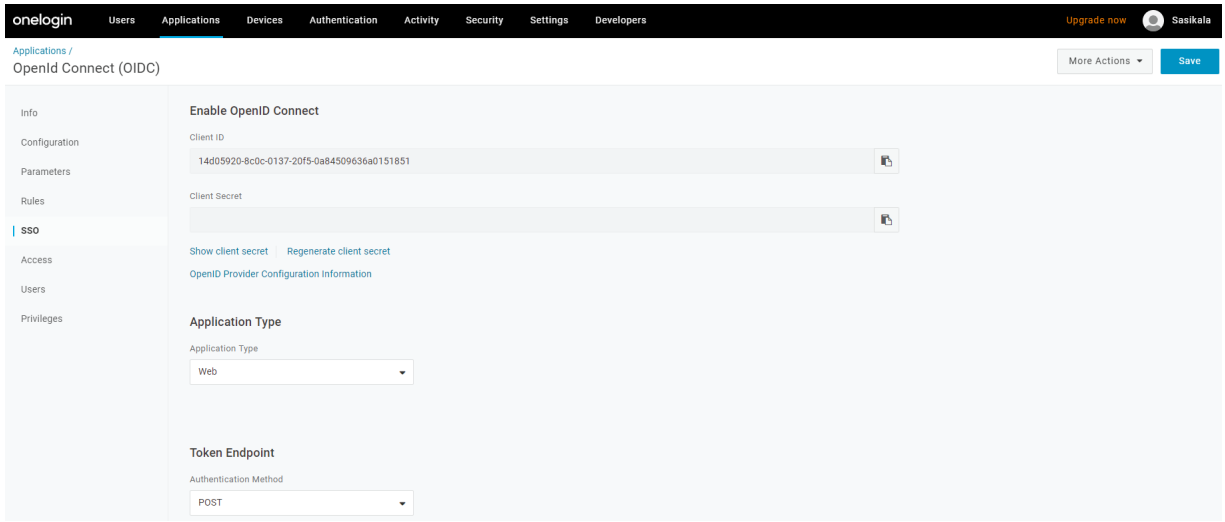


f Konfigurieren Sie Benutzerrollen mit dem Wert „--Keine Transformation--(Einzelwertausgabe) (--No transform--(Single value output))“, die im Gruppenattribut gesendet werden sollen, und klicken Sie auf **Speichern (Save)**.

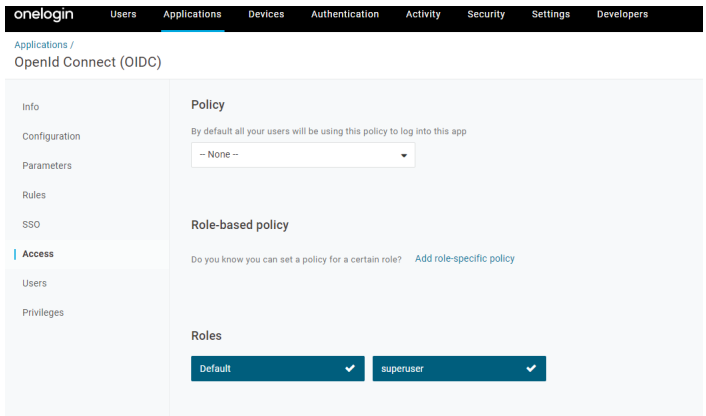
g Wählen Sie auf der Registerkarte **SSO** im Dropdown-Menü**Anwendungstyp (Application Type)** die Option **Web** aus.

h Wählen Sie im Dropdown-Menü **Authentifizierungsmethode (Authentication Method)** die Option **POST** als den Token-Endpoint aus und klicken Sie auf **Speichern (Save)**.

Notieren Sie auch die Clientanmeldedaten (Client-ID und geheimer Clientschlüssel), die während der SSO-Konfiguration in SD-WAN Orchestrator verwendet werden sollen.



i Wählen Sie auf der Registerkarte **Zugriff (Access)** die Rollen aus, die zur Anmeldung berechtigt sind, und klicken Sie auf **Speichern (Save)**.



3 So fügen Sie Ihrer SD-WAN Orchestrator-Anwendung Rollen und Benutzer hinzu:

a Klicken Sie auf **Benutzer (Users)** > **Benutzer (Users)** und wählen Sie einen Benutzer aus.

b Wählen Sie auf der Registerkarte **Anwendung (Application)** im Dropdown-Menü **Rollen (Roles)** auf der linken Seite eine Rolle aus, die dem Benutzer zugeordnet werden soll.

c Klicken Sie auf **Benutzer speichern (Save Users)**.

Ergebnisse

Sie haben die Einrichtung einer OIDC-basierten Anwendung in OneLogin für SSO abgeschlossen.

Nächste Schritte

Konfigurieren Sie Single Sign-On in SD-WAN Orchestrator.

Erstellen einer neuen Rolle in OneLogin

Um eine neue Rolle zu erstellen, führen Sie die Schritte in diesem Verfahren aus.

Verfahren

1. Klicken Sie auf **Benutzer (Users)** > **Rollen (Roles)**.
2. Klicken Sie auf **Neue Rolle (New Role)**.
3. Geben Sie einen Dateinamen für die Rolle ein.

   Wenn Sie zum ersten Mal eine Rolle einrichten, werden auf der Registerkarte **Anwendungen (Applications)** alle Anwendungen in Ihrem Firmenkatalog angezeigt.
4. Klicken Sie auf eine Anwendung, um Sie auszuwählen, und klicken Sie auf **Speichern (Save)**, um die ausgewählten Anwendungen zur Rolle hinzuzufügen.

Erstellen eines neuen Benutzers in OneLogin

Um einen neuen Benutzer zu erstellen, führen Sie die Schritte in diesem Verfahren aus.

Verfahren

1. Klicken Sie auf **Benutzer (Users)** > **Benutzer (Users)** > **Neuer Benutzer (New User)**.

   Der Bildschirm **Neuer Benutzer (New User)** wird angezeigt.
2. Geben Sie alle obligatorischen Details ein, wie Vorname, Nachname und E-Mail-Adresse des Benutzers, und klicken Sie auf **Benutzer speichern (Save User)**.

Konfigurieren von PingIdentity für Single Sign-On

Um eine OpenID Connect (OIDC)-basierte Anwendung in PingIdentity für Single Sign-On (SSO) einzurichten, führen Sie die Schritte in diesem Verfahren aus.

Voraussetzungen

Stellen Sie sicher, dass Sie über ein PingOne-Konto für die Anmeldung verfügen.

Hinweis Zurzeit unterstützt SD-WAN Orchestrator PingOne als Identitätspartner (IDP). Jedes PingIdentity-Produkt, das OIDC unterstützt, kann jedoch einfach konfiguriert werden.

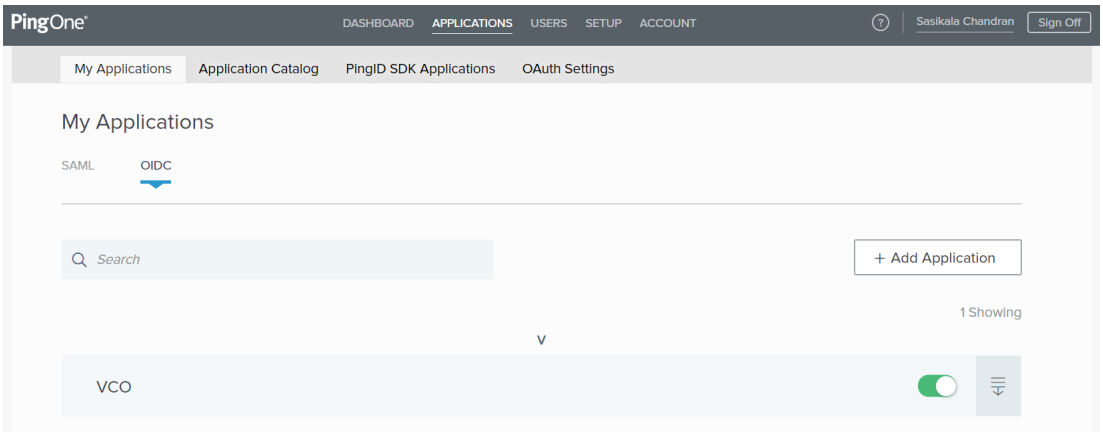
Verfahren

1. Melden Sie sich bei Ihrem PingOne-Konto als Admin-Benutzer an.

   Der **PingOne**-Startbildschirm wird angezeigt.

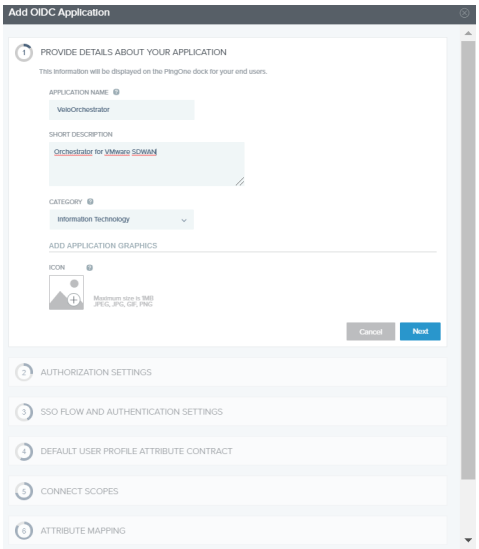
2 So erstellen Sie eine neue Anwendung:

a Klicken Sie in der oberen Navigationsleiste auf **Anwendungen (Applications)**.



b Wählen Sie auf der Registerkarte **Meine Anwendungen (My Applications)** die Option **OIDC** aus und klicken Sie dann auf **Anwendung hinzufügen (Add Application)**.

Das Popup-Fenster **OIDC-Anwendung hinzufügen (Add OIDC Application)** wird angezeigt.



c Geben Sie grundlegende Details wie Name, Kurzbeschreibung und Kategorie für die Anwendung ein und klicken Sie auf **Weiter (Next)**.

d Wählen Sie unter **AUTORISIERUNGSEINSTELLUNGEN (AUTHORIZATION SETTINGS)** den **Autorisierungscode (Authorization Code)** als zulässige Gewährungstypen aus und klicken Sie auf **Weiter (Next)**.

Notieren Sie auch die Erkennungs-URL und die Clientanmeldedaten (Client-ID und geheimer Clientschlüssel), die während der SSO-Konfiguration in SD-WAN Orchestrator verwendet werden sollen.

e Geben Sie unter **SSO-FLOW UND AUTHENTIFIZIERUNGSEINSTELLUNGEN (SSO FLOW AND AUTHENTICATION SETTINGS)** gültige Werte für die Start-SSO-URL und die Weiterleitungs-URL ein und klicken Sie auf **Weiter (Next)**.

In der SD-WAN Orchestrator-Anwendung finden Sie im unteren Bereich des Bildschirms **Authentifizierung konfigurieren (Configure Authentication)** den Link für die Umleitungs-URL. Idealerweise liegt die SD-WAN Orchestrator-Umleitungs-URL in diesem Format vor: https://<Orchestrator-URL>/login/ssologin/openidCallback. Die Start-SSO-URL wird in diesem Format angezeigt: https://<vco>/<Domänenname>/login/doEnterpriseSsoLogin.

f Klicken Sie unter **STANDARD-BENUTZERPROFILATTRIBUT-VERTRAG (DEFAULT USER PROFILE ATTRIBUTE CONTRACT)** auf **Attribut hinzufügen (Add Attribute)**, um weitere Benutzerprofilattribute hinzuzufügen.

g Geben Sie im Textfeld **Attributname (Attribute Name)** *group_membership* ein, aktivieren Sie das Kontrollkästchen **Erforderlich (Required)** und klicken Sie dann auf **Weiter (Next)**.

Hinweis Das Attribut *group_membership* ist erforderlich, um Rollen von PingOne abzurufen.

h Wählen Sie unter **VERBINDUNGSBEREICHE (CONNECT SCOPES)** die Bereiche aus, die für Ihre SD-WAN Orchestrator-Anwendung während der Authentifizierung abgerufen werden können, und klicken Sie auf **Weiter (Next)**.

i Ordnen Sie unter **Attributzuordnung (Attribute Mapping)** die Attribute Ihres Identitätsspeichers den Ansprüchen zu, die Ihrer SD-WAN Orchestrator-Anwendung zur Verfügung stehen.

Hinweis Die für eine funktionierende Integration erforderlichen Mindestzuordnungen sind „email“, „given_name“, „family_name“, „phone_number“, „sub“ und „group_membership“ (zugeordnet zu „memberOf“).

j Wählen Sie unter **Gruppenzugriff (Group Access)** alle Benutzergruppen aus, die Zugriff auf Ihre SD-WAN Orchestrator-Anwendung haben sollen, und klicken Sie auf **Fertig (Done)**.

Die Anwendung wird zu Ihrem Konto hinzugefügt und ist auf dem Bildschirm **Meine Anwendung (My Application)** verfügbar.

Ergebnisse

Sie haben die Einrichtung einer OIDC-basierten Anwendung in PingOne für SSO abgeschlossen.

Nächste Schritte

Konfigurieren Sie Single Sign-On in SD-WAN Orchestrator.

Erstellen einer neuen Benutzergruppe in PingIdentity

Um eine neue Benutzergruppe zu erstellen, führen Sie die Schritte in diesem Verfahren aus.

Verfahren

1 Klicken Sie auf **Benutzer (Users)** > **Benutzerverzeichnis (User Directory)**.

2 Klicken Sie auf der Registerkarte **Gruppen (Groups)** auf **Gruppe hinzufügen (Add Group)**

Der Bildschirm **Neue Gruppe (New Group)** wird angezeigt.

3 Geben Sie im Textfeld **Name** einen Namen für die Gruppe ein und klicken Sie auf **Speichern (Save)**.

Erstellen eines neuen Benutzers in PingIdentity

Um einen neuen Benutzer hinzuzufügen, führen Sie die Schritte in diesem Verfahren aus.

Verfahren

1 Klicken Sie auf **Benutzer (Users)** > **Benutzerverzeichnis (User Directory)**.

2 Klicken Sie auf der Registerkarte **Benutzer (Users)** auf das Dropdown-Menü **Benutzer hinzufügen (Add Users)** und wählen Sie **Neuen Benutzer erstellen (Create New User)** aus.

Der Bildschirm **Benutzer (User)** wird angezeigt.

3 Geben Sie alle obligatorischen Details ein, wie z. B. Benutzername, Kennwort und E-Mail-ID des Benutzers.

4 Klicken Sie unter **Gruppenmitgliedschaften (Group Memberships)** auf **Hinzufügen (Add)**.

Das Popup-Fenster **Gruppenmitgliedschaft hinzufügen (Add Group Membership)** wird angezeigt.

5 Suchen Sie den Benutzer und fügen Sie ihn einer Gruppe hinzu. Klicken Sie dann auf **Speichern (Save)**.

Konfigurieren von Azure Active Directory für Single Sign-On

Um eine OpenID Connect (OIDC)-basierte Anwendung in Microsoft Azure Active Directory (AzureAD) für Single Sign-On (SSO) einzurichten, führen Sie die Schritte in diesem Verfahren aus.

Voraussetzungen

Stellen Sie sicher, dass Sie über ein AzureAD-Konto verfügen.

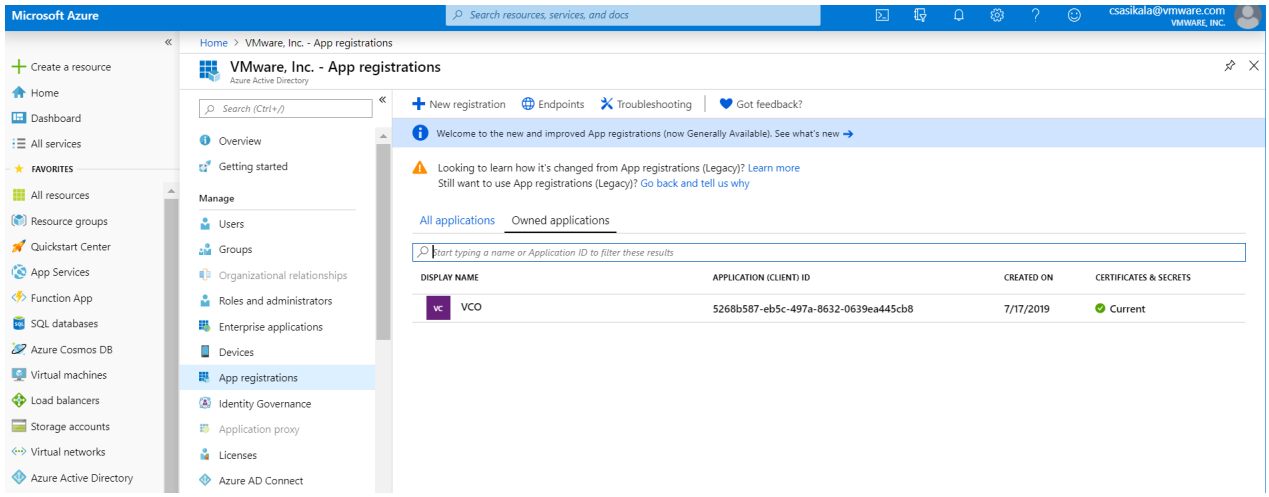
Verfahren

1 Melden Sie sich bei Ihrem Microsoft Azure-Konto als Admin-Benutzer an.

Der **Microsoft Azure**-Startbildschirm wird angezeigt.

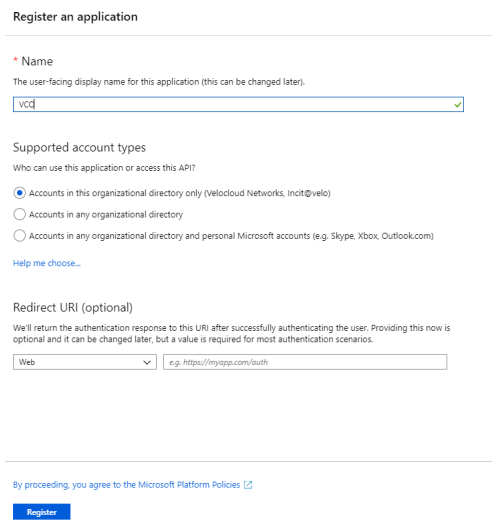
2 So erstellen Sie eine neue Anwendung:

a Suchen Sie nach dem **Azure Active Directory**-Dienst.



b Navigieren Sie zu **App-Registrierung (App registration)** > **Neue Registrierung (New registration)**.

Der Bildschirm **Anwendung registrieren (Register application)** wird angezeigt.



c Geben Sie im Feld **Name** den Namen für Ihre SD-WAN Orchestrator-Anwendung ein.

d Geben Sie im Feld **Umleitungs-URL (Redirect URL)** die Umleitungs-URL ein, die Ihre SD-WAN Orchestrator-Anwendung als Callback-Endpoint verwendet.

In der SD-WAN Orchestrator-Anwendung finden Sie im unteren Bereich des Bildschirms **Authentifizierung konfigurieren (Configure Authentication)** den Link für die Umleitungs-URL. Idealerweise liegt die SD-WAN Orchestrator-Umleitungs-URL in diesem Format vor: https://<Orchestrator-URL>/login/ssologin/openidCallback.

e Klicken Sie auf **Registrieren (Register)**.

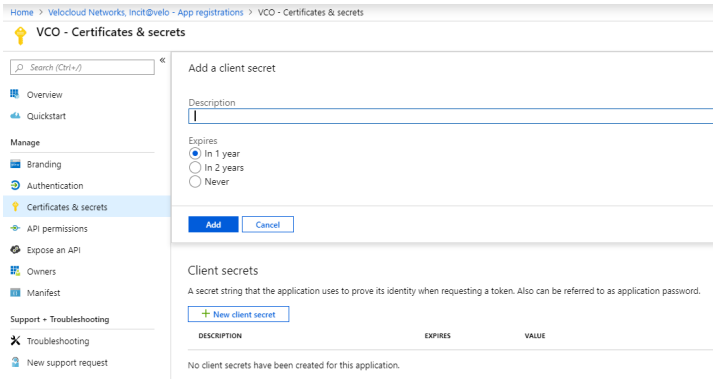
Ihre SD-WAN Orchestrator-Anwendung wird registriert und auf den Registerkarten **Alle Anwendungen (All applications)** und **Eigene Anwendungen (Owned applications)** angezeigt. Stellen Sie sicher, dass Sie die Client-ID/Anwendungs-ID notieren, die während der SSO-Konfiguration in SD-WAN Orchestrator verwendet werden soll.

f Klicken Sie auf **Endpoints** und kopieren Sie die bekannte OIDC-Konfigurations-URL, die während der SSO-Konfiguration in SD-WAN Orchestrator verwendet werden soll.

g Um einen geheimen Clientschlüssel für Ihre SD-WAN Orchestrator-Anwendung zu erstellen, klicken Sie auf der Registerkarte **Eigene Anwendungen (Owned applications)** auf Ihre SD-WAN Orchestrator-Anwendung.

h Navigieren Sie zu **Zertifikate und geheime Schlüssel (Certificates & secrets)** > **Neuer geheimer Schlüssel (New client secret)**.

Der Bildschirm **Neuen geheimen Clientschlüssel hinzufügen (Add a client secret)** wird angezeigt.

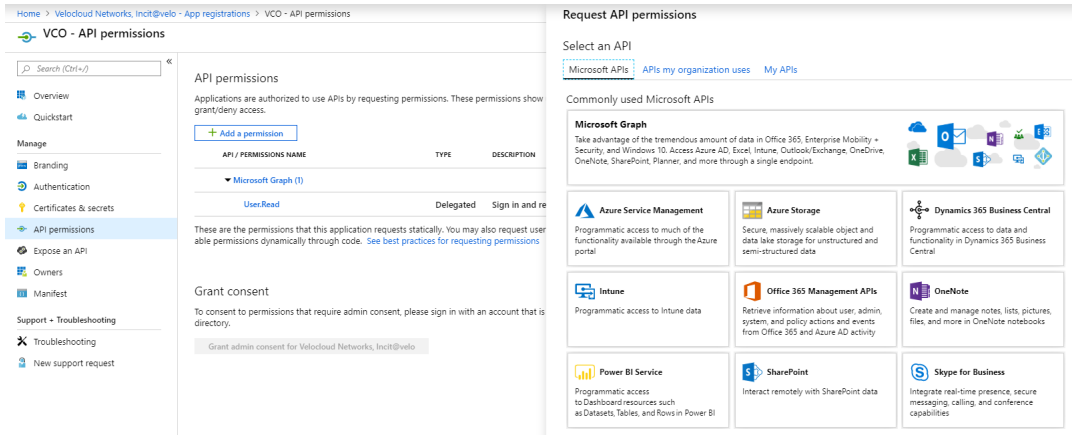


i Geben Sie Details wie Beschreibung und Ablaufwert des geheimen Schlüssels an und klicken Sie auf **Hinzufügen (Add)**.

Der geheime Clientschlüssel wird für die Anwendung erstellt. Notieren Sie den Wert für den neuen geheimen Clientschlüssel, der während der SSO-Konfiguration in SD-WAN Orchestrator verwendet wird.

j Um die Berechtigungen für Ihre SD-WAN Orchestrator-Anwendung zu konfigurieren, klicken Sie auf Ihre SD-WAN Orchestrator-Anwendung und navigieren Sie zu **API-Berechtigungen (API permissions)** > **Berechtigung hinzufügen (Add a permission)**.

Der Bildschirm **API-Berechtigungen anfordern (Request API permissions)** wird angezeigt.



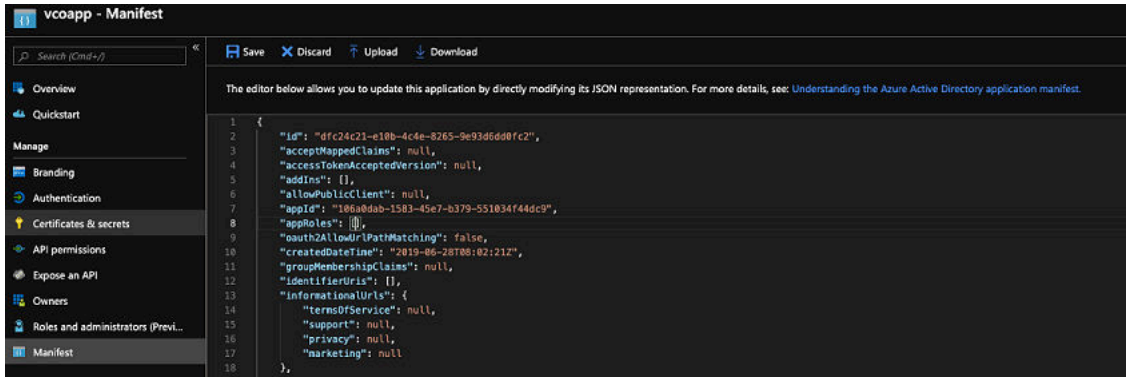
k Klicken Sie auf **Microsoft-Diagramm (Microsoft Graph)** und wählen Sie **Anwendungsberechtigungen (Application permissions)** als Berechtigungstyp für Ihre Anwendung aus.

l Wählen Sie unter **Berechtigungen auswählen (Select permissions)** im Dropdown-Menü **Verzeichnis (Directory)** den Eintrag **Directory.Read.All** und aus dem Dropdown-Menü **Benutzer (User)** den Eintrag **User.Read.All** aus.

m Klicken Sie auf **Berechtigungen hinzuzufügen (Add permissions)**.

n Um Rollen im Manifest hinzuzufügen und zu speichern, klicken Sie auf Ihre SD-WAN Orchestrator-Anwendung und klicken Sie im Anwendungsbildschirm **Übersicht (Overview)** auf **Manifest**.

Ein webbasierter Manifest-Editor wird geöffnet, sodass Sie das Manifest im Portal bearbeiten können. Optional können Sie **Herunterladen (Download)** auswählen, um das Manifest lokal zu bearbeiten, und dann **Hochladen (Upload)** verwenden, um es erneut auf Ihre Anwendung anzuwenden.

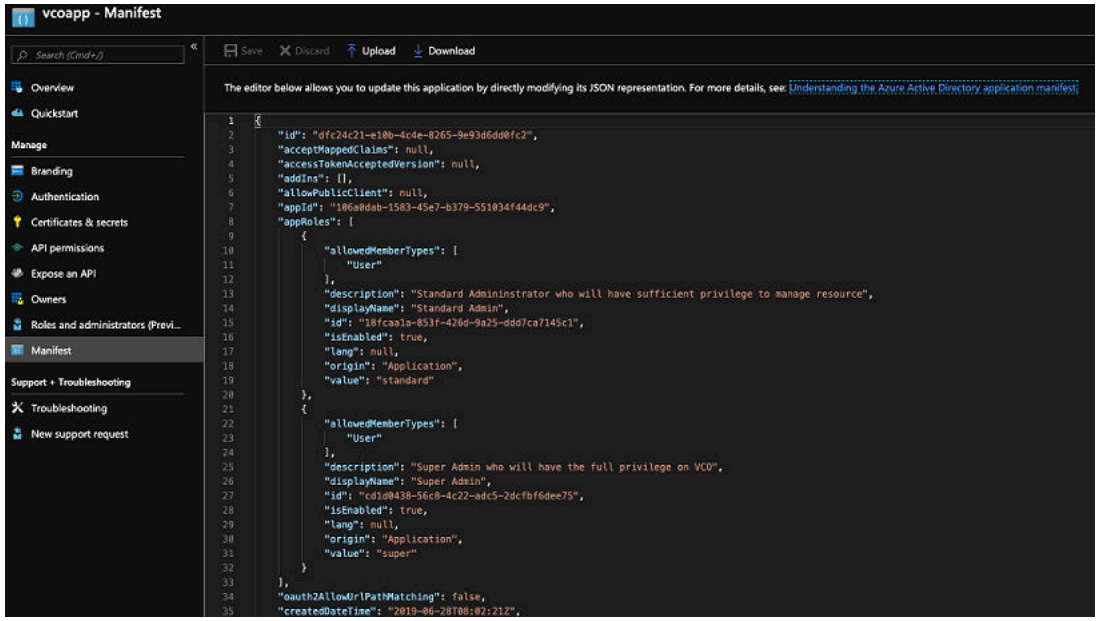


o Suchen Sie im Manifest nach dem `appRoles`-Array und fügen Sie ein oder mehrere Rollenobjekte hinzu, wie im folgenden Beispiel dargestellt, und klicken Sie auf **Speichern (Save)**.

Beispiele für Rollenobjekte

```
{
            "allowedMemberTypes": [
                "User"
            ],
            "description": "Standard Administrator who will have sufficient privilege to
manage resource",
            "displayName": "Standard Admin",
            "id": "18fcaa1a-853f-426d-9a25-ddd7ca7145c1",
            "isEnabled": true,
            "lang": null,
            "origin": "Application",
            "value": "standard"
        },
        {
            "allowedMemberTypes": [
                "User"
            ],
            "description": "Super Admin who will have the full privilege on SD-WAN
Orchestrator",
            "displayName": "Super Admin",
            "id": "cd1d0438-56c8-4c22-adc5-2dcfbf6dee75",
            "isEnabled": true,
```

```
            "lang": null,
            "origin": "Application",
            "value": "superuser"
        }
```



Hinweis Stellen Sie sicher, dass `id` auf einen neu generierten GUID-Wert festgelegt wird.

3 So weisen Sie Ihrer SD-WAN Orchestrator-Anwendung Gruppen und Benutzer zu:

a Navigieren Sie zu **Azure Active Directory** > **Unternehmensanwendungen (Enterprise applications)**.

b Suchen Sie nach der SD-WAN Orchestrator-Anwendung und wählen Sie sie aus.

c Klicken Sie auf **Benutzer und Gruppen (Users and groups)** und weisen Sie der Anwendung Benutzer und Gruppen zu.

d Klicken Sie auf **Übermitteln (Submit)**.

Ergebnisse

Sie haben die Einrichtung einer OIDC-basierten Anwendung in AzureAD für SSO abgeschlossen.

Nächste Schritte

Konfigurieren Sie Single Sign-On in SD-WAN Orchestrator.

Erstellen eines neuen Gastbenutzers in AzureAD

Um einen neuen Gastbenutzer zu erstellen, führen Sie die Schritte in diesem Verfahren aus.

Verfahren

1 Navigieren Sie zu **Azure Active Directory** > **Benutzer (Users) Alle Benutzer (All users)**.

2 Klicken Sie auf **Neuer Gastbenutzer (New Guest User)**.

Das Popup-Fenster **Neuer Gastbenutzer (New Guest User)** wird angezeigt.

3 Geben Sie im Textfeld **E-Mail-Adresse (Email address)** die E-Mail-Adresse des Gastbenutzers ein und klicken Sie auf **Einladen (Invite)**.

Der Gastbenutzer erhält sofort eine anpassbare Einladung, mit der er sich bei seinem Zugriffsbereich anmelden kann.

4 Gastbenutzer im Verzeichnis können Anwendungen oder Gruppen zugewiesen werden.

Konfigurieren von VMware CSP für Single Sign-On

Um VMware Cloud Services Platform (CSP) für Single Sign-On (SSO) zu konfigurieren, führen Sie die Schritte in diesem Verfahren aus.

Voraussetzungen

Melden Sie sich bei der VMware CSP-Konsole (Bereitstellungs- oder Produktionsumgebung) mit Ihrer VMware-Konto-ID an. Wenn Sie neu bei VMware Cloud sind und noch kein VMware-Konto haben, können Sie bei der Anmeldung ein Konto erstellen. Weitere Informationen finden Sie im Abschnitt „Anmelden bei VMware CSP“ in der Dokumentation Verwenden von VMware Cloud.

Verfahren

1 Wenden Sie sich an den VMware SD-WAN-Supportanbieter, um einen Einladungs-URL-Link zur Registrierung Ihrer SD-WAN Orchestrator-Anwendung bei VMware CSP zu erhalten. Informationen zur Kontaktaufnahme mit dem Supportanbieter finden Sie unter https://kb.vmware.com/s/article/53907 und https://www.vmware.com/support/contacts/us_support.html.

Der VMware SD-WAN-Supportanbieter erstellt und teilt Folgendes:

- Eine Diensteinladungs-URL, die für Ihre Kundenorganisation eingelöst werden muss
- Eine Dienstdefinitions-UUID und ein Dienstrollenname, die für die Rollenzuordnung in Orchestrator verwendet werden sollen

2 Lösen Sie die Einladungs-URL für Ihre bestehende Kundenorganisation ein oder erstellen Sie eine neue Kundenorganisation, indem Sie die Schritte auf dem Benutzeroberflächen-Bildschirm befolgen.

Sie müssen ein Organisationsbesitzer sein, um die Diensteinladungs-URL für Ihre bestehende Kundenorganisation einzulösen.

3 Nachdem Sie die Einladung für den Dienst eingelöst haben, können Sie bei der Anmeldung bei der VMware CSP-Konsole die Anwendungskachel im Bereich **Meine Dienste (My Services)** auf der Seite **VMware Cloud Services** anzeigen.

   Die Organisation, bei der Sie angemeldet sind, wird in der Menüleiste unter Ihrem Benutzernamen angezeigt. Notieren Sie sich die ID der Organisation, indem Sie auf Ihren Benutzernamen klicken, der bei der Konfiguration von Orchestrator verwendet werden soll. Eine verkürzte Version der ID wird unter dem Organisationsnamen angezeigt. Klicken Sie auf die ID, um die vollständige Organisations-ID anzuzeigen.

4 Melden Sie sich bei der VMware CSP-Konsole an und erstellen Sie eine OAuth-Anwendung. Die Schritte dazu finden Sie unter Verwenden von OAuth 2.0 für Web-Apps. Legen Sie den Umleitungs-URI unbedingt auf die im Bildschirm **Authentifizierung konfigurieren (Configure Authentication)** in Orchestrator angezeigte URL fest.

   Nachdem die OAuth-Anwendung in der VMware CSP-Konsole erstellt wurde, notieren Sie sich die IDP-Integrationsdetails wie Client-ID und geheimen Clientschlüssel. Diese Details werden für die Konfiguration von SSO in Orchestrator benötigt.

5 Melden Sie sich bei Ihrer SD-WAN Orchestrator-Anwendung als Super-Admin-Benutzer an und konfigurieren Sie SSO mithilfe der IDP-Integrationsdetails wie folgt.

   a Klicken Sie auf **Verwaltung (Administration)** > **Systemeinstellungen (System Settings)**.

      Der Bildschirm **Systemeinstellungen (System Settings)** wird angezeigt.

   b Klicken Sie auf die Registerkarte **Allgemeine Informationen (General Information)** und geben Sie im Textfeld **Domäne (Domain)** den Domänennamen für Ihr Unternehmen ein, sofern er noch nicht festgelegt ist.

      Hinweis Um die SSO-Authentifizierung für die SD-WAN Orchestrator-Instanz zu aktivieren, müssen Sie den Domänennamen für Ihr Unternehmen einrichten.

   c Klicken Sie auf die Registerkarte **Authentifizierung (Authentication)** und wählen Sie im Dropdown-Menü **Authentifizierungsmodus (Authentication Mode)** den Eintrag **SSO** aus.

   d Wählen Sie im Dropdown-Menü **Identitätsanbietervorlage (Identity Provider template)** die Option **VMwareCSP** aus.

   e Geben Sie im Textfeld **Organisations-ID (Organization Id)** die Organisations-ID (die Sie in Schritt 3 notiert haben) im folgenden Format ein: */csp/gateway/am/api/orgs/ <vollständige Organisations-ID>*.

   f Geben Sie im Textfeld **Bekannte URL für die Konfiguration von OIDC (OIDC well-known config URL)** die OpenID Connect (OIDC)-Konfigurations-URL (https://console.cloud.vmware.com/csp/gateway/am/api/.well-known/openid-configuration) für Ihren Identitätsanbieter ein.

      In der SD-WAN Orchestrator-Anwendung werden Endpoint-Details, wie z. B. Aussteller, Autorisierungs-Endpoint, Token-Endpoint und Benutzerinformations-Endpoint, für Ihren IDP automatisch befüllt.

g Geben Sie im Textfeld **Client-ID (Client Id)** die Client-ID ein, die Sie im Schritt zur Erstellung der OAuth-Anwendung notiert haben.

h Geben Sie im Textfeld **Geheimer Clientschlüssel (Client Secret)** den Code für den geheimen Clientschlüssel ein, den Sie im Schritt zur Erstellung der OAuth-Anwendung notiert haben.

i Um die Rolle des Benutzers in SD-WAN Orchestrator zu ermitteln, wählen Sie entweder **Standardrolle verwenden (Use Default Role)** oder **Identitätsanbieterrollen verwenden (Use Identity Provider Roles)** aus.

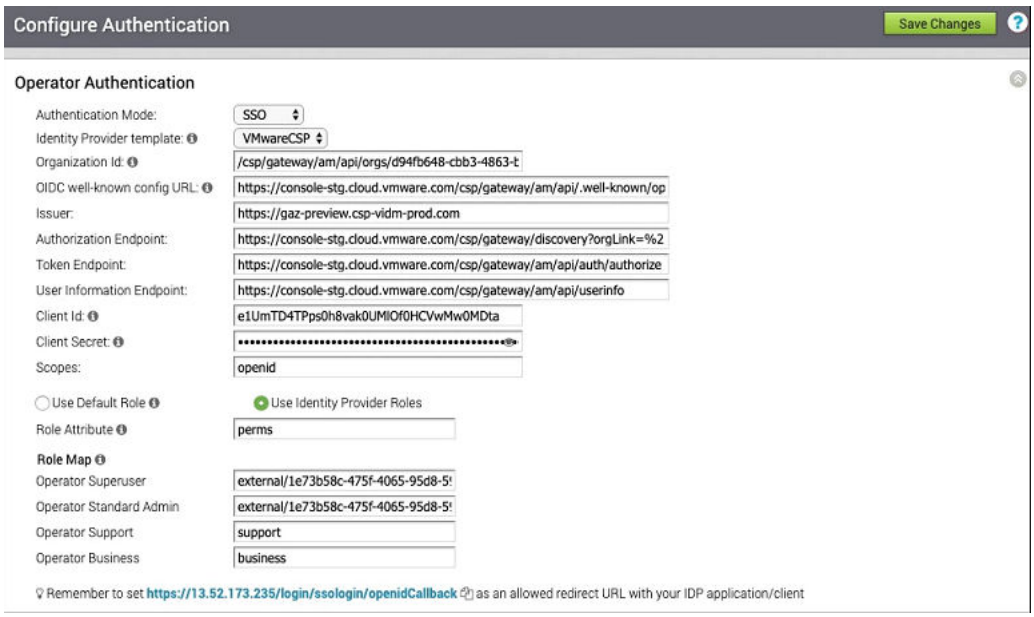
j Geben Sie bei Auswahl der Option **Identitätsanbieterrollen verwenden (Use Identity Provider Roles)** im Textfeld **Rollenattribut (Role Attribute)** den Namen des Attributs ein, das in VMware CSP festgelegt ist, um Rollen zurückzugeben.

k Ordnen Sie im Bereich **Rollenzuordnung (Role Map)** die von VMwareCSP bereitgestellten Rollen zu allen SD-WAN Orchestrator-Rollen zu, die durch Kommas getrennt sind.

Rollen in VMware CSP haben folgendes Format: external/<Dienstdefinitions-UUID>/<Name der Dienstrolle, der bei der Erstellung der Dienstvorlage erwähnt wurde>. Verwenden Sie dieselbe Dienstdefinitions-UUID und denselben Dienstrollennamen, den Sie von Ihrem Supportanbieter erhalten haben.

6 Klicken Sie auf **Änderungen speichern (Save Changes)**, um die SSO-Konfiguration zu speichern.

7 Klicken Sie auf **Konfiguration testen (Test Configuration)**, um die eingegebene OIDC-Konfiguration (OpenID Connect) zu validieren.



Der Benutzer wird zur VMware CSP-Website geleitet und kann die Zugangsdaten eingeben. Nach der IDP-Verifizierung und erfolgreichen Weiterleitung zum SD-WAN Orchestrator-Test-Callback wird eine erfolgreiche Validierungsmeldung angezeigt.

Ergebnisse

Sie haben die Integration der SD-WAN Orchestrator-Anwendung in VMware CSP für SSO abgeschlossen und können auf die SD-WAN Orchestrator-Anwendung zugreifen, indem Sie sich bei der VMware CSP-Konsole anmelden.

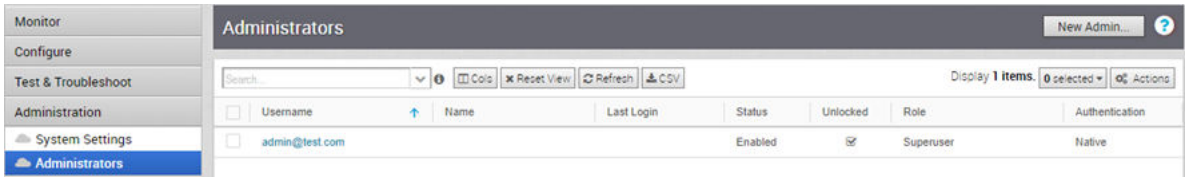
Nächste Schritte

- Verwalten Sie die Benutzer innerhalb der Organisation, indem Sie neue Benutzer hinzufügen und den Benutzern die entsprechende Rolle zuweisen. Weitere Informationen finden Sie unter Verwalten von Benutzern.

Verwalten von Admin-Benutzern

Auf der Seite **Administratoren (Administrators)** werden die vorhandenen Admin-Benutzer angezeigt. Standard-Admin-Superuser und Standard-Admins können neue Admin-Benutzer mit verschiedenen Rollenrechten erstellen und API-Token für jeden Admin-Benutzer konfigurieren.

Klicken Sie im Unternehmensportal auf **Verwaltung (Administration) > Administratoren (Administrators)**.



Klicken Sie auf **Aktionen (Actions)**, um die folgenden Aktivitäten auszuführen:

- **Neuer Admin (New Admin)**: Erstellt neue Admin-Benutzer. Weitere Informationen finden Sie unter Erstellen von neuen Admin-Benutzern.
- **Admin ändern (Modify Admin)**: Ändert die Eigenschaften des ausgewählten Admin-Benutzers. Sie können auch auf den Link zum Benutzernamen klicken, um die Eigenschaften zu ändern. Weitere Informationen finden Sie unter Konfigurieren von Admin-Benutzern.
- **Kennwort zurücksetzen (Password Reset)**: Sendet eine E-Mail an den ausgewählten Benutzer mit einem Link zum Zurücksetzen des Kennworts.
- **Admin löschen (Delete Admin)**: Löscht die ausgewählten Benutzer.

Erstellen von neuen Admin-Benutzern

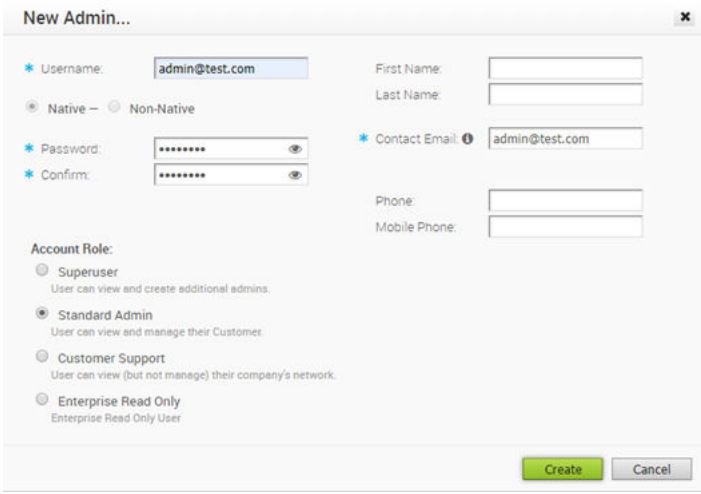
Standardadministrator-Superuser und Standardadministratoren können neue Admin-Benutzer erstellen.

Klicken Sie im Unternehmensportal auf **Verwaltung (Administration) > Administratoren (Administrators)**.

Verfahren

1 Sie können neue Admin-Benutzer erstellen, indem Sie entweder auf **Neuer Admin (New Admin)** oder **Aktionen (Actions) > Neuer Admin (New Admin)** klicken.

2 Geben Sie im Fenster **Neuer Admin (New Admin)** die folgenden Details ein:



   a Geben Sie die Benutzerdetails wie Benutzername, Kennwort, Name, E-Mail und Telefonnummern ein.

   b Wenn Sie den Authentifizierungsmodus als „Nativ (Native)“ in Konfigurieren der Unternehmensauthentifizierung ausgewählt haben, wird der Typ des Benutzers als „Nativ (Native)“ ausgewählt. Wenn Sie einen anderen Authentifizierungsmodus ausgewählt haben, können Sie den Benutzertyp festlegen. Wenn Sie „Nicht nativ“ für den Benutzer auswählen, steht die Kennwortoption nicht zur Verfügung, da sie vom Authentifizierungsmodus vererbt wird.

   c **Kontorolle (Account Role)**: Wählen Sie eine Benutzerrolle in den verfügbaren Optionen aus.

3 Klicken Sie auf **Erstellen (Create)**.

Ergebnisse

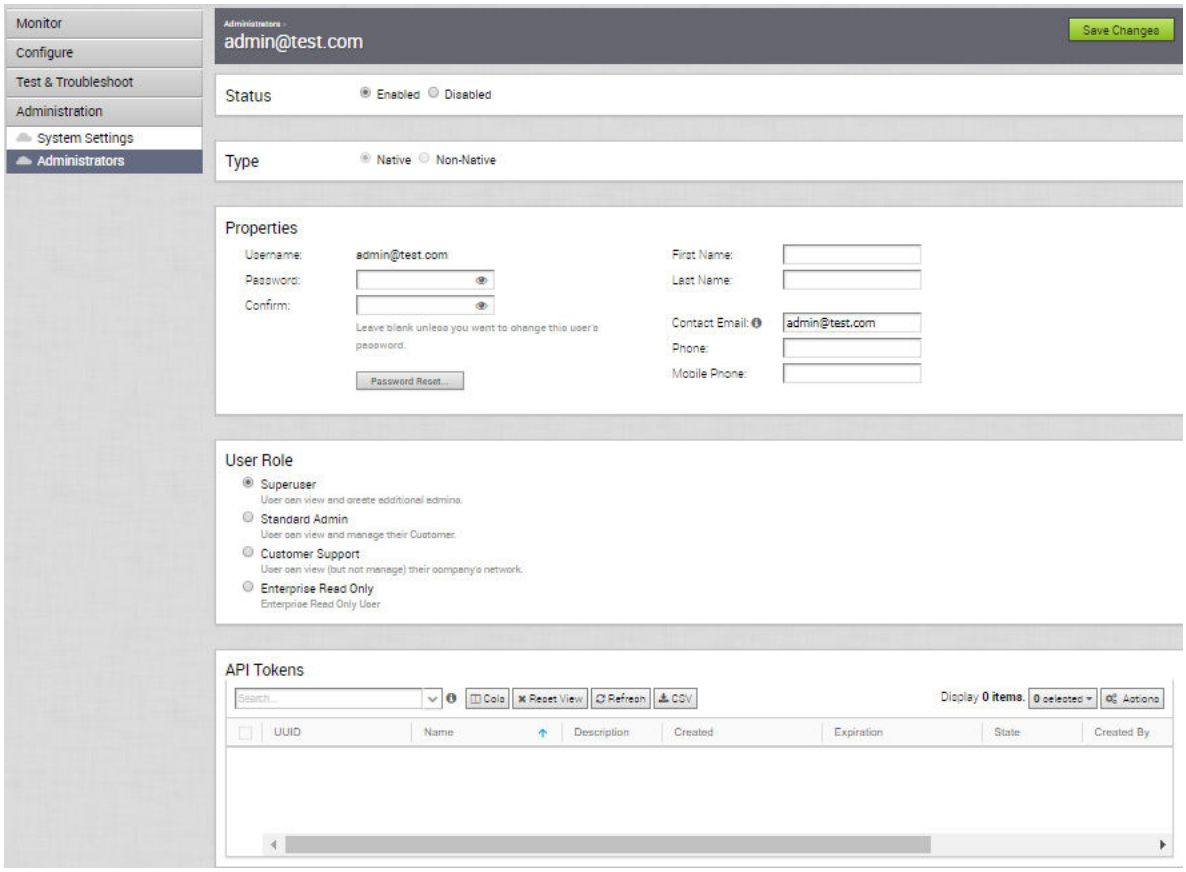
Die Benutzerdetails werden auf der Seite **Administratoren (Administrators)** angezeigt.

Konfigurieren von Admin-Benutzern

Sie können zusätzliche Einstellungen konfigurieren und API-Token für einen Admin-Benutzer erstellen.

Klicken Sie im Unternehmensportal auf **Verwaltung (Administration) > Administratoren (Administrators)**. Um einen Admin-Benutzer zu konfigurieren, klicken Sie auf den Link zu einem Benutzernamen oder wählen Sie den Benutzer aus und klicken Sie auf **Aktionen (Actions) > Admin ändern (Modify Admin)**.

Die vorhandenen Eigenschaften des ausgewählten Benutzers werden angezeigt. Gegebenenfalls können Sie Folgendes hinzufügen oder ändern:



Status

Standardmäßig lautet der Status auf **Aktiviert (Enabled)**. Bei Auswahl von **Deaktiviert (Disabled)** wird der Benutzer von allen aktiven Sitzungen abgemeldet.

Typ (Type)

Wenn Sie den Authentifizierungsmodus als **Nativ (Native)** unter Konfigurieren der Unternehmensauthentifizierung ausgewählt haben, wird der Typ des Benutzers als **Nativ (Native)** ausgewählt. Wenn Sie einen anderen Authentifizierungsmodus ausgewählt haben, können Sie den Benutzertyp festlegen. Wenn Sie **Nicht nativ (Non-Native)** für den Benutzer auswählen, können Sie weder das Kennwort zurücksetzen noch die Benutzerrolle ändern.

Eigenschaften (Properties)

Die vorhandenen Kontaktdetails des Benutzers werden angezeigt. Sie können die Details gegebenenfalls ändern und das Kennwort zurücksetzen. Wenn Sie auf **Kennwort zurücksetzen (Password Reset)** klicken, wird eine E-Mail mit einem Link zum Zurücksetzen des Kennworts an den Benutzer gesendet.

Rolle (Role)

Der vorhandene Typ der Benutzerrolle wird angezeigt. Sie können gegebenenfalls eine andere Rolle für den Benutzer auswählen. Die Rollenberechtigungen ändern sich entsprechend.

API-Token (API Tokens)

Die Benutzer können anstelle der sitzungsbasierten Authentifizierung mithilfe von Token auf die Orchestrator-APIs zugreifen. Als Operator-Superuser können Sie die API-Token für die Kunden verwalten. Sie können mehrere API-Token für einen Benutzer erstellen.

Für Enterprise Read Only- und MSP Business Specialist-Benutzer ist tokenbasierte Authentifizierung nicht aktiviert.

API-Token konfigurieren (Configure API Tokens)

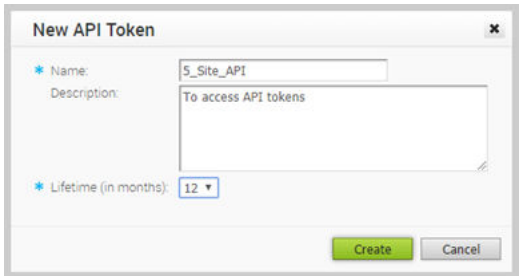
Alle Benutzer können Token basierend auf den Berechtigungen erstellen, die ihren Benutzerrollen zugewiesen wurden. Ausgenommen hiervon sind Enterprise Read Only- und MSP Business Specialist-Benutzer.

Die Benutzer können die folgenden Aktionen basierend auf ihren Rollen ausführen:

- Enterprise-Benutzer können Token für sie erstellen, herunterladen und widerrufen.
- Operator-Superuser können Token anderer Operator- und Enterprise-Benutzer verwalten, wenn der Enterprise-Benutzer Benutzerberechtigungen an den Operator delegiert hat.
- Enterprise-Superuser können die Token aller Benutzer in diesem Unternehmen verwalten.
- Benutzer können nur ihre eigenen und nicht die Token anderer Benutzer herunterladen.
- Superuser können die Token für andere Benutzer nur erstellen und widerrufen.

So verwalten Sie die API-Token:

- Klicken Sie im Abschnitt **API-Token (API Tokens)** auf **Aktionen (Actions) > Neues API-Token (New API Token)**, um ein neues Token zu erstellen.
- Geben Sie im Fenster **Neues API-Token (New API Token)** in den Feldern **Name** und **Beschreibung (Description)** Werte für das Token ein und wählen Sie im Dropdown-Menü die **Lebensdauer (Lifetime)** aus.



- Klicken Sie auf **Erstellen (Create)**. Das neue Token wird im Raster **API-Token (API Tokens)** angezeigt.

- Anfänglich wird der Status des Tokens als **Ausstehend (Pending)** angezeigt. Zum Herunterladen des Tokens wählen Sie es aus und klicken auf **Aktionen (Actions) > API-Token herunterladen (Download API Token)**. Der Status ändert sich in **Aktiviert (Enabled)**. Dies bedeutet, dass das API-Token für den Zugriff auf die API verwendet werden kann.
- Zum Deaktivieren eines Tokens wählen Sie es aus und klicken auf **Aktionen (Actions) > API-Token widerrufen (Revoke API Token)**. Der Status des Token wird als **Widerrufen (Revoked)** angezeigt.
- Nach Ablauf der Lebensdauer des Tokens ändert sich der Status in **Abgelaufen (Expired)**.

Nur der mit dem Token verknüpfte Benutzer kann das Token herunterladen. Nach dem Herunterladen wird nur die ID des Tokens angezeigt. Sie können ein Token nur einmal herunterladen.

Nach dem Herunterladen kann der Benutzer das Token als Teil des Autorisierungs-Headers der Anforderung senden, um auf die Orchestrator-API zuzugreifen.

Das folgende Beispiel zeigt einen Beispielausschnitt des Codes für den Zugriff auf eine API.

```
curl –k –H "Authorization: Token <Token>"
  –X POST https://vco/portal/
  –d '{ "id": 1, "jsonrpc": "2.0", "method": "enterprise/getEnterpriseUsers", "params":
{ "enterpriseId": 1 }}'
```

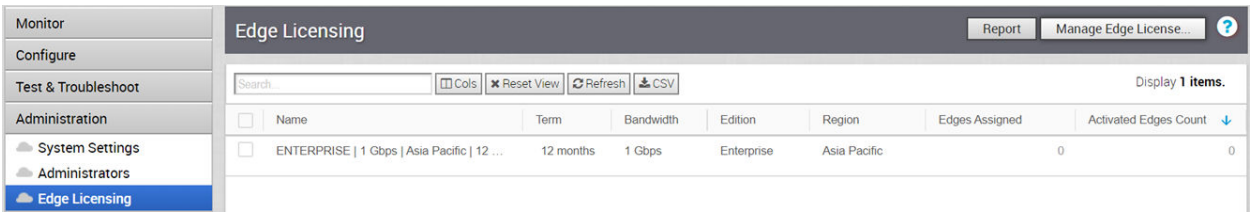
Klicken Sie nach dem Ändern der Einstellungen und der API-Token auf **Änderungen speichern (Save Changes)**.

Edge-Lizenzierung

SD-WAN Orchestrator stellt verschiedene Lizenzen für die Edges bereit. Standardadministrator-Superuser, Standardadministratoren, Unternehmensexperten und Benutzer des Kundensupports können einen Bericht mit den ihnen zugewiesenen Lizenzen anzeigen und erzeugen.

Klicken Sie im Unternehmens-Portal auf **Verwaltung (Administration) > Edge-Lizenzierung (Edge Licensing)**.

Hinweis Die Registerkarte **Edge-Lizenzierung (Edge Licensing)** steht nur dann zur Verfügung, wenn der Operator Edge-Lizenzierung aktiviert und dem Enterprise-Kunden die Lizenzen zugewiesen hat.



Klicken Sie auf **Bericht (Report)**, um einen Bericht zu den Lizenzen und den verknüpften Edges im MS Excel-Format anzuzeigen.

So weisen Sie einem Edge eine Lizenz zu:

- Klicken Sie im Unternehmensportal auf **Konfigurieren (Configure) > Edges**.
- Um jedem Edge eine Lizenz zuzuweisen, klicken Sie auf den Link zu dem Edge und wählen Sie die Lizenz auf der Seite **Edge – Übersicht (Edge Overview)** aus. Sie können auch den Edge auswählen und auf **Aktionen (Actions) > Edge-Lizenz zuweisen (Assign Edge License)** klicken, um die Lizenz zuzuweisen.
- Wählen Sie zum Zuweisen einer Lizenz zu mehreren Edges den entsprechenden Edge aus, klicken Sie auf **Aktionen (Actions) > Edge-Lizenz zuweisen (Assign Edge License)** und wählen Sie die Lizenz aus.

Weitere Informationen finden Sie unter Kapitel 15 Registerkarte „Edge-Übersicht (Edge Overview)“.

Konfigurieren der SD-WAN Edge-Hochverfügbarkeit

24

In diesem Abschnitt wird beschrieben, wie Hochverfügbarkeit auf einem SD-WAN Edge aktiviert wird.

Dieses Kapitel enthält die folgenden Themen:

Übersicht über SD-WAN Edge HA

Beim SD-WAN Edge handelt es sich um die VMware SD-WAN-Datenebenenkomponente, die am Standort der Zweigstelle des Benutzers bereitgestellt wird. Im Hochverfügbarkeitsmodus (HA-Modus) konfigurierte SD-WAN Edges-Instanzen sind gegenseitige Spiegelungen und werden im SD-WAN Orchestrator als einzelner SD-WAN Edge angezeigt.

Es gibt zwei Optionen bei der Konfiguration im HA-Modus:

1 HA-Option 1

2 HA-Option 2

Eine Beschreibung der beiden Optionen finden Sie unter *Hochverfügbarkeitsoptionen (High Availability, HA)*.

In diesem Dokument werden die Schritte beschrieben, die zum Aktivieren der Hochverfügbarkeit (HA) und zum Einrichten eines zweiten SD-WAN Edge als Standbygerät für einen aktivierten Edge erforderlich sind.

Voraussetzungen

In diesem Abschnitt werden HA-Anforderungen beschrieben, die erfüllt sein müssen, bevor ein SD-WAN Edge als Standby konfiguriert wird.

- Bei den beiden SD-WAN Edges-Instanzen muss es sich um das gleiche Modell handeln.
- Es sollte nur ein SD-WAN Edge im SD-WAN Orchestrator bereitgestellt sein.
- Auf dem Standby-SD-WAN Edge darf keine bestehende Konfiguration vorhanden sein.

Hochverfügbarkeitsoptionen

Edges können als einzelnes Standalone-Gerät installiert oder mit einem anderen Edge gekoppelt werden, um Unterstützung für Hochverfügbarkeit bereitzustellen. Die HA-Konfiguration ist nur für kabelgebundene WAN-Verbindungen vorgesehen.

HA-Optionen

Bei der Konfiguration im HA-Modus stehen zwei Optionen zur Verfügung (Option 1 und Option 2). Beide Optionen werden im Folgenden beschrieben.

Überlegungen zu HA

Überlegungen zu beiden HA-Optionen:

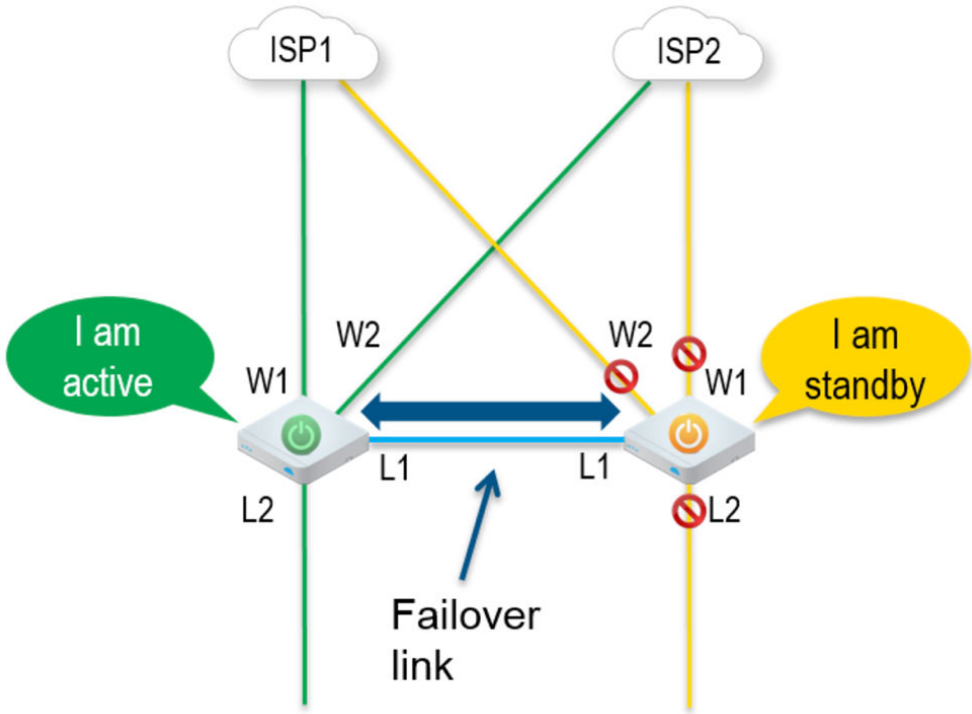
- Edges wählen automatisch Option 1 oder Option 2 aus. Edges wählen Option 1 aus, wenn beide Edges mit denselben WAN-Links verknüpft sind. Edges wählen Option 2 aus, wenn die Edges erkennen, dass sie mit verschiedenen WAN-Links verbunden sind.
- Beide Optionen werden auf allen SD-WAN Edge-Plattformen unterstützt: 510, 520, 520v, 540, 840, 2000 und Virtual Edge.
- HA wird nur zwischen den identischen SD-WAN Edge-Plattformmodellen unterstützt (siehe https://www.velocloud.com/get-started/ für die verschiedenen Edge-Plattformmodelle).

HA-Option 1: Standard-HA

In diesem Abschnitt wird die HA-Option 1 „Standard-HA (Standard HA)“ beschrieben.

Topologieübersicht für HA-Option 1

Die folgende Abbildung zeigt eine konzeptionelle Übersicht über die HA-Option 1.



Die Edges, ein aktiver und ein Standby-Edge, sind über L1-Ports verbunden, um einen Failover-Link zu erstellen. Der Standby-SD-WAN Edge blockiert alle Ports mit Ausnahme des L1-Ports für den Failover-Link.

Voraussetzungen für die HA-Option 1

- Die LAN-seitigen Switches in den folgenden Konfigurationsbeschreibungen müssen STP-fähig und mit STP konfiguriert sein.
- Darüber hinaus müssen LAN- und WAN-Ports des SD-WAN Edge mit unterschiedlichen L2-Switches verbunden sein. Wenn die Ports mit demselben Switch verbunden werden müssen, müssen die LAN- und WAN-Ports isoliert werden.
- Die beiden SD-WAN Edges-Instanzen müssen gespiegelte physische WAN- und LAN-Verbindungen aufweisen.

Bereitstellungstypen für HA-Option 1

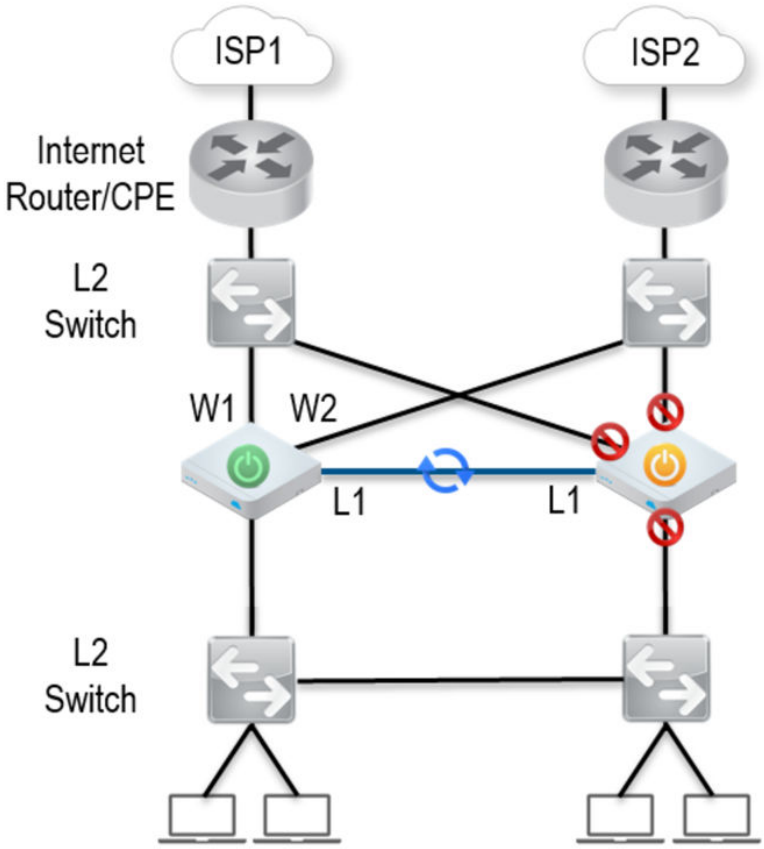
HA-Option 1 verfügt über zwei mögliche Bereitstellungstypen:

- Bereitstellungstyp 1 nutzt L2-Switches
- Bereitstellungstyp 2 nutzt eine Kombination aus L2- und L3-Switches

In den folgenden Abschnitten werden diese beiden Bereitstellungstypen beschrieben.

Bereitstellungstyp 1: Hochverfügbarkeit (HA, High Availability) mithilfe von L2-Switches

Die folgende Abbildung zeigt die Netzwerkverbindungen, die ausschließlich L2-Switches verwenden.



W1 und W2 sind WAN-Verbindungen, die zum Herstellen einer Verbindung mit dem L2-Switch verwendet werden, um WAN-Konnektivität mit ISPs bereitzustellen. Der L1-Link stellt eine Verbindung zu den beiden SD-WAN Edges-Instanzen her und wird für Keepalive und Kommunikation zwischen den SD-WAN Edges-Instanzen zur Unterstützung von HA verwendet. Die LAN-Verbindungen des SD-WAN Edge werden verwendet, um eine Verbindung mit den L2-Switches der Zugriffsebene herzustellen.

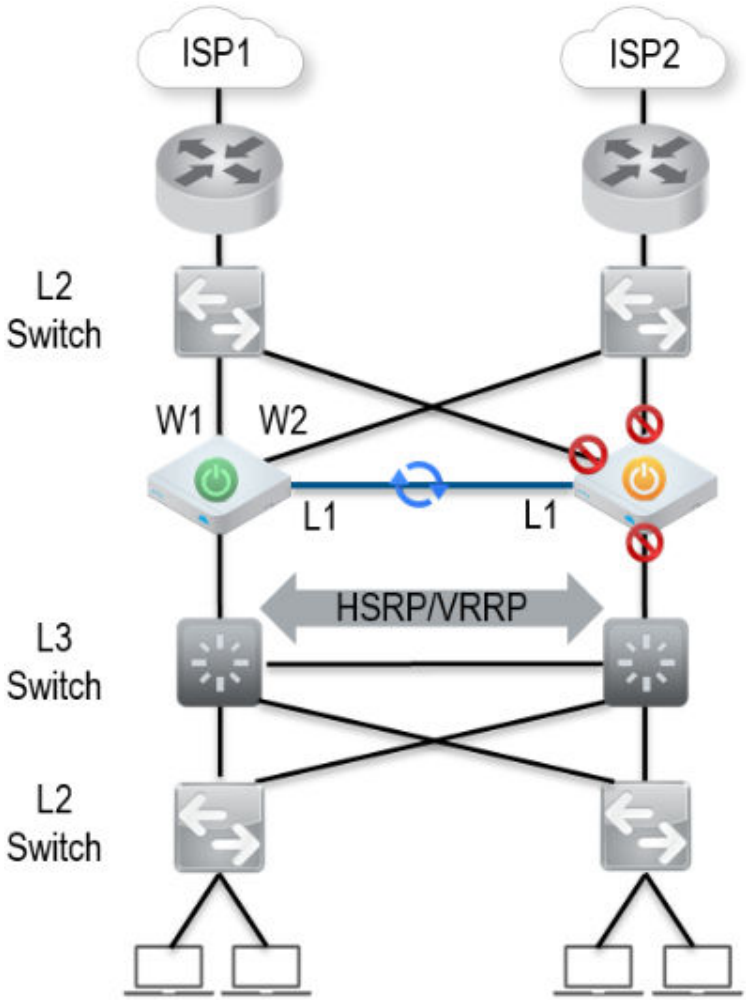
Überlegungen für Bereitstellungstyp 1

- Der gleiche ISP-Link muss mit demselben Port auf beiden Edges verbunden sein.
- Verwenden Sie den L2-Switch, um denselben ISP-Link für beide Edges zur Verfügung zu stellen.
- Der Standby-SD-WAN Edge stört den Datenverkehr nicht, indem er alle zugehörigen Ports mit Ausnahme des Failover-Links (L1-Port) blockiert.
- Die Sitzungsinformationen werden über den Failover-Link zwischen dem aktiven und dem Standby-SD-WAN Edges synchronisiert.

- Wenn der aktive Edge den Ausfall eines LAN-Links erkennt, erfolgt ebenfalls ein Failover auf den Standby-Edge, wenn dieser einen aktiven LAN-Link aufweist.

Bereitstellungstyp 2: Hochverfügbarkeit (HA, High Availability) mithilfe von L2/L3-Switches

Die folgende Abbildung zeigt die Netzwerkverbindungen, die L2- und L3-Switches verwenden.



Die SD-WAN Edge-WAN-Verbindungen (W1 und W2) werden zum Herstellen einer Verbindung mit L2-Switches verwendet, um jeweils für ISP1 und ISP2 eine WAN-Verbindung bereitzustellen. Die L1-Verbindungen auf den SD-WAN Edges-Instanzen sind verbunden, um einen Failover-Link für HA-Unterstützung bereitzustellen. Die LAN-Verbindungen des VMware SD-WAN Edge werden zum Herstellen einer Verbindung mit L2-Switches verwendet, die mit mehreren Endbenutzergeräten verbunden sind.

Überlegungen für Bereitstellungstyp 2

- HSRP/VRRP ist auf dem L3-Switch-Paar erforderlich.
- Die statische Route des SD-WAN Edge zeigt auf die HSRP-VIP des L3-Switches als nächsten Hop zur Erreichung der Endstationen hinter L2-Switches.

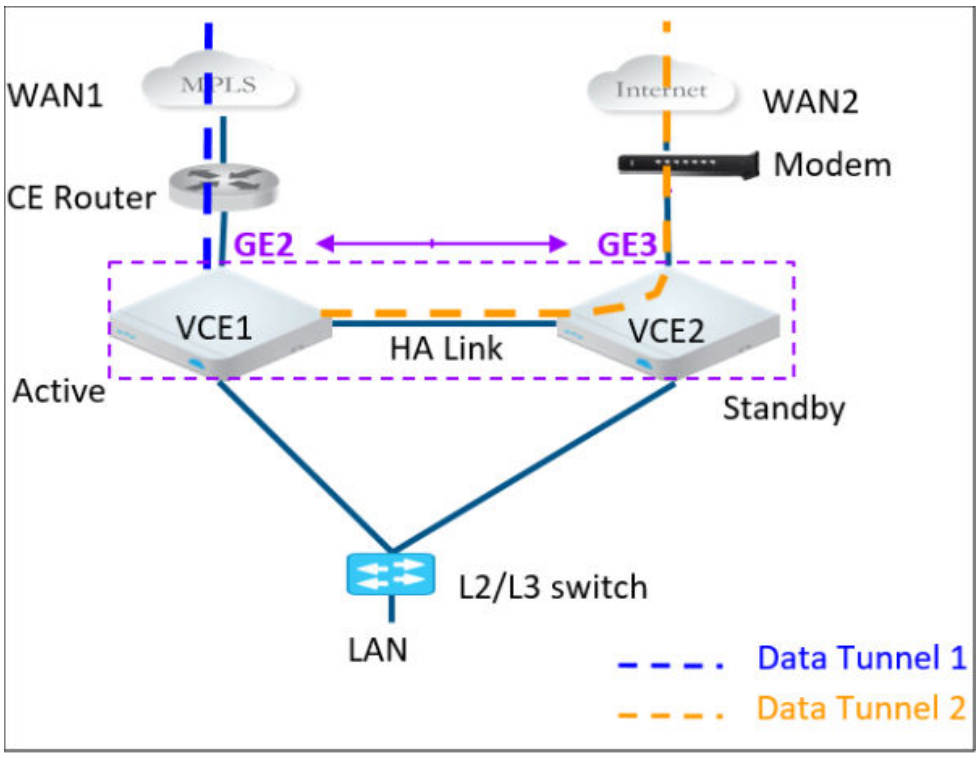
- Der gleiche ISP-Link muss mit demselben Port auf beiden SD-WAN Edges-Instanzen verbunden sein. Der L2-Switch muss denselben ISP-Link für beide Edges zur Verfügung stellen.
- Der Standby-SD-WAN Edge stört den Datenverkehr nicht, indem er alle zugehörigen Ports außer dem Failover-Link (L1-Port) blockiert.
- Die Sitzungsinformationen werden über den Failover-Link zwischen dem aktiven und dem Standby-SD-WAN Edges synchronisiert.
- Das HA-Paar führt bei Erkennung des L1-Ausfalls der LAN-/WAN-Links ebenfalls ein Failover vom aktiven auf den Standby-Edge durch.
  - Wenn der aktive und Standby-Edge dieselbe Anzahl an aktiven LAN-Links aufweisen, der Standby-Edge aber über eine größere Anzahl an aktiven WAN-Links verfügt, findet ein Switchover auf den Standby-Edge statt.
  - Wenn der Standby-Edge eine größere Anzahl an LAN-Links und mindestens einen WAN-Link aufweist, findet ein Failover auf den Standby-Edge statt. In dieser Situation wird davon ausgegangen, dass der Standby-Edge LAN-seitig über mehr Benutzer als der aktive Edge verfügt und der Standby-Edge mehr LAN-seitigen Benutzern erlaubt, eine Verbindung mit dem WAN herzustellen, vorausgesetzt, WAN-Konnektivität steht zur Verfügung.

HA-Option 2: Erweiterte HA

In diesem Abschnitt werden Optionen für die HA-Option 2 „Erweiterte HA (Enhanced HA)“ beschrieben

Bei Verwendung der HA-Option 2 werden L2-Switches auf der WAN-Seite der Edges nicht mehr benötigt. Diese Option wird ausgewählt, wenn der aktive Edge mit dem Standby-Edge verbundene WAN-Links erkennt, die sich von denjenigen unterscheiden, mit denen er selbst verbunden ist.

Die folgende Abbildung zeigt eine konzeptionelle Übersicht über die HA-Option 2.



Die Edges, ein aktiver und ein Standby-Edge, sind über L1-Ports verbunden, um einen Failover-Link zu erstellen. Der Standby-SD-WAN Edge blockiert alle Ports mit Ausnahme des L1-Ports für den Failover-Link. Wie in der Abbildung gezeigt, richtet der aktive Edge Overlay-Tunnel auf beiden WAN-Links ein (die mit ihm selbst und dem Standby-Edge verbunden sind).

Hinweis Die beiden SD-WAN Edges-Instanzen sollten keine gespiegelten physischen WAN-Verbindungen aufweisen. Wie in der Abbildung gezeigt, kann VCE2 GE2 nicht als WAN-Link verwenden, wenn VCE1 GE2 bereits als WAN-Link nutzt.

Um den mit dem Standby-Edge verbundenen WAN-Link nutzen zu können, richtet der aktive Edge den Overlay-Tunnel über den HA-Link ein. Der Datenverkehr aus dem LAN wird an den aktiven Edge weitergeleitet. In der Unternehmensrichtlinie für den Branch wird die Verteilung des Datenverkehrs auf die Overlay-Tunnel festgelegt.

Split-Brain-Bedingung

Wenn die HA-Verbindung getrennt wird oder wenn Aktiv- und Standby-Edge nicht miteinander kommunizieren können, übernehmen beide Edges die aktive Rolle. Infolgedessen beginnen beide Edges, auf ARP-Anfragen auf ihren LAN-Schnittstellen zu antworten. Dies hat zur Folge, dass der LAN-Datenverkehr an beide Edges weitergeleitet wird, was zu übergreifenden Baumschleifen im LAN führen könnte.

Normalerweise führen Switches das Spanning-Tree-Protokoll aus, um Schleifen im Netzwerk zu verhindern. In einem solchen Zustand würde der Switch den Datenverkehr zu einem oder beiden Edges blockieren. Dies würde zu einem Gesamtverlust des Datenverkehrs durch das Edge-Paar führen.

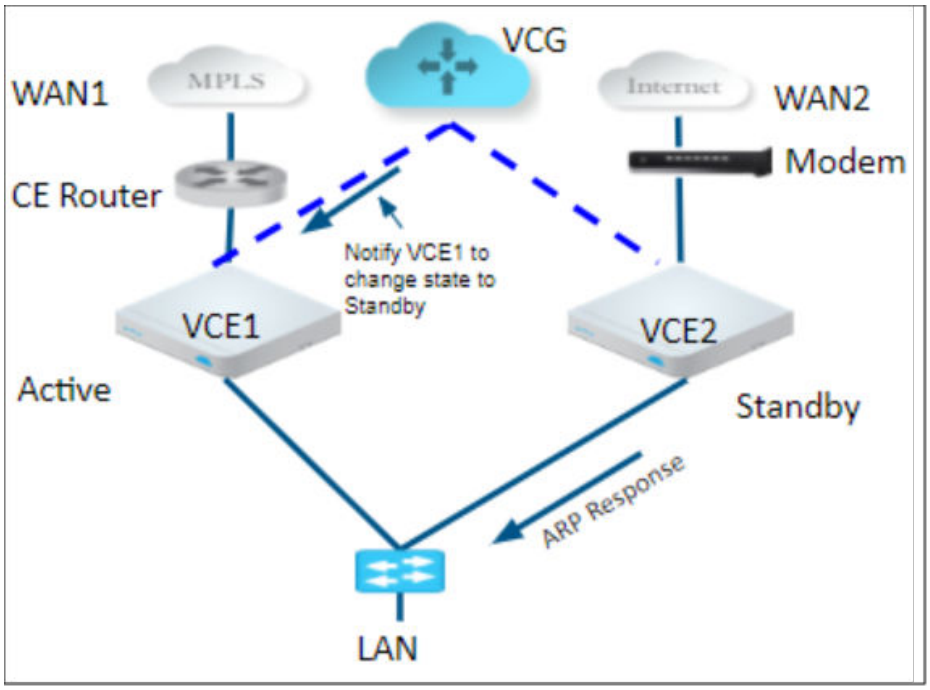
Hinweis Der Tunnel zum primären Gateway ist eine Voraussetzung für die Split-Brain-Erkennung. Daher sollte in WAN 2 ein Tunnel zu SD-WAN Gateway vorhanden sein.

Split-Brain-Erkennung und Prävention

Das primäre Gateway wird verwendet, um Split-Brain-Bedingungen zu verhindern.

Das Gateway verfügt über eine bereits vorhandene Verbindung zum aktiven Edge. In einer Split-Brain-Bedingung wird der Status des Standby-Edge in „Aktiv“ geändert, und es wird versucht, einen Tunnel zum Gateway einzurichten. Das Gateway sendet eine Antwort zurück an den Standby-Edge und weist ihn an, in den Standby-Modus zu wechseln. Außerdem wird die Einrichtung des Tunnels nicht zugelassen. Das Gateway verfügt immer über Tunnel nur vom aktiven Edge. Nur die LAN-Schnittstellen bleiben blockiert (solange das HA-Kabel ausgefallen ist). Wie in der folgenden Abbildung gezeigt, signalisiert das Gateway VCE1, um in den Standby-Modus im LAN zu wechseln. Dadurch wird logisch verhindert, dass das Split-Brain-Szenario eintritt.

Hinweis Das normale Failover von „Aktiv“ zu „Standby“ in einem Split-Brain-Szenario ist nicht mit dem normalen Failover identisch. Es kann einige zusätzliche Millisekunden/Sekunden dauern, bis die Konvergenz erreicht ist.



Ausfallszenarien

In diesem Abschnitt werden die folgenden Szenarien beschrieben, die ein Failover vom aktiven zum Standby-Edge auslösen können.

- Ausfall des WAN-Links
- Ausfall des LAN-Links
- Edge-Funktionen reagieren nicht
- Absturz des Edge oder Neustart oder keine Reaktion

Unterstützung für BGP über HA-Verbindung

Falls die Edges zu der erweiterten HA-Option wechseln, tauscht der aktive SD-WAN Edge die BGP-Routen über die HA-Verbindung aus. BGP auf dem aktiven Edge kann jetzt eine Nachbarschaft mit einem Peer einrichten, der nur mit der WAN-Verbindung des Standby-Edge verbunden ist.

Dadurch erhält der aktive Edge die Möglichkeit, Routen von der/den WAN-Verbindung(en), die mit dem Standby-Edge verbunden sind, zu lernen. Der Routing-Daemon auf Standby wird in keine der Funktionen einbezogen. Der Standby-Edge selbst führt nur einen Passthrough durch.

Hinweis Routen werden zwischen den aktiven und den Standby-Edges nicht synchronisiert. Wenn also im obigen Szenario ein Failover stattfindet und ein Standby-Edge aktiv wird, richtet der BGP-Daemon auf dem neu aktiven Edge eine neue Nachbarschaft mit demselben BGP-Peer ein.

Auswahlkriterien zur Bestimmung des aktiven und Standby-Status

In diesem Abschnitt werden die Auswahlkriterien zur Bestimmung des aktiven und Standby-Modus beschrieben.

- Suchen Sie nach einem Edge mit einer höheren Anzahl an LAN-Schnittstellen (L2 und L3). Der Edge mit der höheren Anzahl an LAN-Schnittstellen wird als „Aktiv (Active)“ ausgewählt. Beachten Sie, dass die für den HA-Link verwendete Schnittstelle nicht als LAN-Schnittstelle gezählt wird.
- Wenn beide Edges dieselbe Anzahl an LAN-Schnittstellen aufweisen, wird der Edge mit der höheren Anzahl an WAN-Schnittstellen als „Aktiv (Active)“ ausgewählt.

Hinweis Es findet keine vorzeitige Entfernung statt, wenn beide Edges dieselbe Anzahl an LAN- und WAN-Schnittstellen aufweisen.

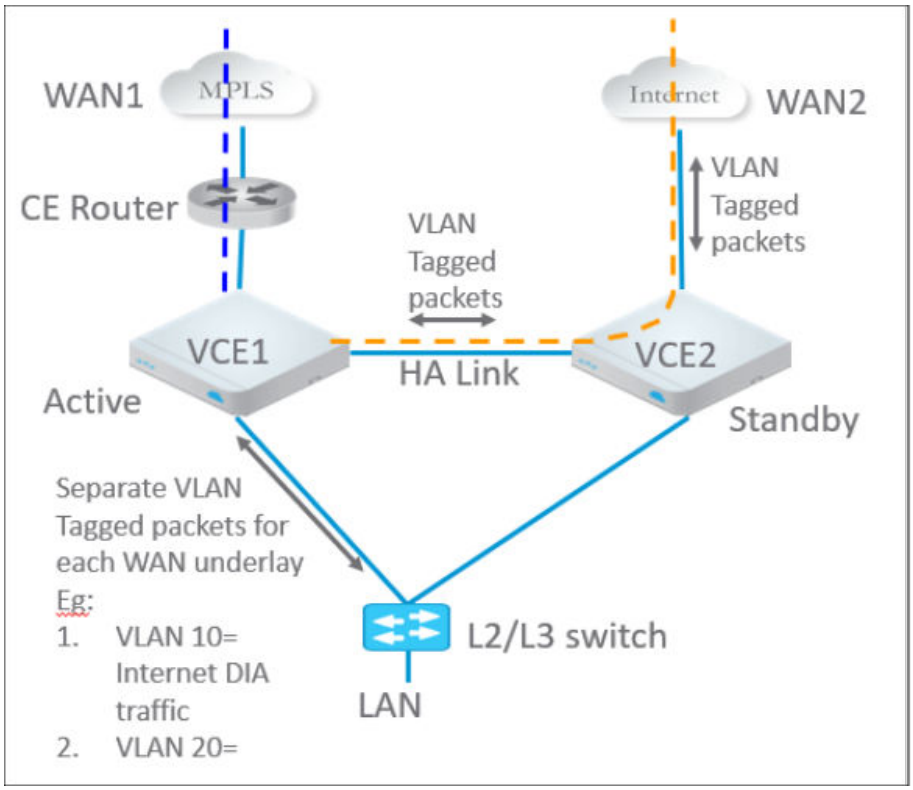
- Zusätzliche Supportmatrix:
  - Statische/DHCP-/PPPoE-Links werden unterstützt.

- Mehrere WAN-Links, die jeweils mit einer separaten VLAN-ID auf einer einzelnen Schnittstelle (z. B. Unterschnittstellen) gekennzeichnet sind, werden unterstützt.
- USB-Modems werden auf HA nicht empfohlen. Die Schnittstelle wird nicht verwendet, wenn sie sich auf dem Standby-Edge befindet.

VLAN-gekennzeichneter Datenverkehr über HA-Verbindung

In diesem Abschnitt wird der VLAN-gekennzeichnete Datenverkehr über eine HA-Verbindung beschrieben.

- Der Internetdatenverkehr von ISP2 ist VLAN-gekennzeichnet.
- Der Kunde verfügt über separate VLANs für den Unternehmensdatenverkehr gegenüber dem DIA-Datenverkehr.
- Die WAN-Verbindung auf dem Standby hat untergeordnete Schnittstellen für den Internetdatenverkehr.
- Mehrere Segmente



Konfigurieren von HA

Um HA (High Availability) zu konfigurieren, konfigurieren Sie die aktiven und Standby-Edges.

Aktivieren von Hochverfügbarkeit (High Availability, HA)

So aktivieren Sie die HA-Funktion im SD-WAN Orchestrator:

1 Wechseln Sie im Navigationsbereich zu **Konfigurieren (Configure) > Edges**.

2 Wählen Sie den SD-WAN Edge aus und klicken Sie dann auf die Registerkarte **Gerät (Device)**.

3 Klicken Sie im Bereich **Hochverfügbarkeit (High Availability)** auf **Aktiv/Standby-Paar (Active Standby Pair)**.

Standardmäßig wird die GE1- oder LAN1-Schnittstelle als HA-Schnittstelle für die Verbindung des Paars je nach SD-WAN Edge-Modell verwendet.

Hinweis Diese Option ist als Edge-Überschreibung verfügbar und kann auf der Profilebene nicht konfiguriert werden. Stellen Sie keine Verbindung mit dem Standby-SD-WAN Edge her.

Warten Sie, bis SD-WAN Edge aktiv ist

Warten Sie nach dem Aktivieren der Hochverfügbarkeitsfunktion in SD-WAN Orchestrator, bis der vorhandene SD-WAN Edge eine aktive Rolle übernimmt, und warten Sie, bis die SD-WAN Orchestrator-Ereignisse als **Hochverfügbarkeit wird aktiviert (High Availability Going Active)** angezeigt werden.

Verbinden des Standy-SD-WAN Edge mit dem aktiven Edge

1 Schalten Sie den Standby-SD-WAN Edge ohne Netzwerkverbindungen ein.

2 Nach dem Hochfahren verbinden Sie die LAN1/GE1-Schnittstelle (wie auf der Registerkarte **Gerät (Device)** angegeben) mit derselben Schnittstelle auf dem aktiven SD-WAN Edge.

3 Warten Sie, bis der aktive SD-WAN Edge den Standby-SD-WAN Edge automatisch erkannt und aktiviert hat. Unter „SD-WAN Orchestrator-Ereignisse (Events)“ wird **HA-Standby aktiviert (HA Standby Activated)** angezeigt, wenn die SD-WAN Orchestrator-Instanz den Standby-SD-WAN Edge erfolgreich aktiviert hat.

Der Standby-Edge startet dann die Synchronisierung mit dem aktiven SD-WAN Edge und wird während des Vorgangs automatisch neu gestartet.

Hinweis Es kann bis zu 10 Minuten dauern, bis sich der Standby-SD-WAN Edge mit dem aktiven Edge synchronisiert und seine Software aktualisiert.

i	Fri Nov 18, 14:37:27	High Availability Ready	[redacted]	Notice	Standby state ready for failover
i	Fri Nov 18, 14:37:25	Edge service startup	[redacted]	Notice	VeloCloud edge service started
i	Fri Nov 18, 14:37:08	Edge online	[redacted]	Info	Management Daemon Started, version 2.2.1 build R221-20161109-GA
i	Fri Nov 18, 14:36:25	HA Peer State Unknown	[redacted]	Notice	Peer state unknown
i	Fri Nov 18, 14:34:59	Standby device software update started	[redacted]	Info	Begin HA Standby update with new software version
i	Fri Nov 18, 14:32:15	High Availability Ready	[redacted]	Notice	Standby state ready for failover
i	Fri Nov 18, 14:32:14	Edge service startup	[redacted]	Notice	VeloCloud edge service started

Verbinden von LAN- und WAN-Schnittstellen auf dem Standby-SD-WAN Edge

Verbinden Sie die LAN- und WAN-Schnittstellen auf dem Standby-SD-WAN Edge und spiegeln Sie die Netzwerkkonnektivität auf dem aktiven Edge.

Unter „SD-WAN Orchestrator-Ereignisse (Events)“ wird **Aktualisierung der Standby-Gerätesoftware abgeschlossen (Standby device software update completed)** angezeigt. Nach Abschluss dieses Vorgangs wird der **HA-Status (HA State)** auf der Seite **Überwachen (Monitor) > Edges** grün angezeigt.

Details zu HA-Ereignissen

In diesem Abschnitt werden die HA-Ereignisse beschrieben.

HA-Ereignis (HA Event)	Beschreibung (Description)
HA_GOING_ACTIVE	Ein Standby-SD-WAN Edge wechselt in den Status „Aktiv (Active)“, da kein Taktsignal vom Peer empfangen wurde.
HA_STANDBY_ACTIVATED	Wenn ein neuer Standby-Edge vom aktiven Edge erkannt wird, aktiviert der aktive Edge den Edge, indem er dieses Ereignis an den SD-WAN Orchestrator sendet. Bei einer erfolgreichen Antwort synchronisiert der aktive Edge die Konfigurationen und Daten.
HA_FAILED	Dies geschieht in der Regel, nachdem sich das HA-Paar gebildet hat und der aktive SD-WAN Edge keine Signale mehr vom Standby-SD-WAN Edge empfängt. Wenn der Standby-SD-WAN Edge beispielsweise neu startet, erhalten Sie diese Nachricht.
HA_READY	Bedeutet, dass der aktive SD-WAN Edge jetzt Signale vom Standby-SD-WAN Edge empfängt. Sobald der Standby-SD-WAN Edge wieder verfügbar ist und das Taktsignal erneut einrichtet, erhalten Sie diese Nachricht.

HA_TERMINATED	Wenn die HA-Konfiguration deaktiviert und erfolgreich auf die Edges angewendet wurde, wird dieses Ereignis erzeugt.
HA_ACTIVATION_FAILURE	Wenn der SD-WAN Orchestrator die HA-Aktivierung nicht überprüfen kann, wird dieses Ereignis generiert. Zu den Beispielen gehören: ■ Der SD-WAN Orchestrator kann kein Zertifikat generieren ■ Hochverfügbarkeit wurde deaktiviert (selten)

VMware SD-WAN Virtual Edge-Bereitstellung

25

Der Virtual Edge ist als virtuelle Maschine verfügbar, die auf Standard-Hypervisoren installiert werden kann. In diesem Abschnitt werden die Voraussetzungen und der Installationsvorgang für die Bereitstellung eines VMware SD-WAN Virtual Edge auf KVM- und VMware ESXi-Hypervisoren erläutert.

Dieses Kapitel enthält die folgenden Themen:

Bereitstellungsvoraussetzungen für den virtuellen VMware SD-WAN Edge

Beschreibt die Anforderungen für die Bereitstellung des virtuellen VMware SD-WAN Edge.

Anforderungen an den virtuellen Edge

Für einen virtuellen Edge benötigen Sie Folgendes:

- 2 x Intel vCPUs mit AES-NI-Befehlssatz
- 4 GB Arbeitsspeicher
- Virtuelle Festplatte (ca. 8 GB Festplattenspeicher)
- 3 bis 8 vNICs (Standard sind 2 x L2-Schnittstellen und 6 x L3-Schnittstellen)

Empfohlene Serverspezifikationen

Netzwerkkarten-Chipsatz	Hardware	Spezifikation
Intel 82599/82599ES	HP DL380G9	http://www.hp.com/hpinfo/newsroom/press_kits/2014/ComputeEra/HP_ProLiantDL380_DataSheet.pdf
Intel X710/XL710	Dell PowerEdge R640	https://www.dell.com/en-us/work/shop/povw/poweredge-r640 ■ CPU-Modell und Kerne – Dual Sockel Intel(R) Xeon(R) Gold 5218 CPU @ 2,30 GHz mit jeweils 16 Kernen ■ Arbeitsspeicher – 384 GB RAM
Intel X710/XL710	Supermicro SYS-6018U-TRTP+	https://www.supermicro.com/en/products/system/1U/6018/SYS-6018U-TRTP_.cfm ■ CPU-Modell und Kerne – Dual Socket Intel(R) Xeon(R) CPU E5-2630 v4 @ 2,20 GHz mit jeweils 10 Kernen ■ Arbeitsspeicher – 256 GB RAM

Empfohlene Netzwerkkartenspezifikationen

Hardwarehersteller	Firmwareversion	Hosttreiber für Ubuntu 16.04/18.04	Hosttreiber für ESXi 6.7
Dual Port Intel Corporation Ethernet Controller XL710 für 40GbE QSFP+	6.80	2.7.11	1.7.17
Dual Port Intel Corporation Ethernet Controller X710 für 10GbE SFP+	6.80	2.7.11	1.7.17
Quad Port Intel Corporation Ethernet Controller X710 für 10GbE SFP+	6.80	2.7.11	1.7.17

Unterstützte Gastbetriebssysteme

- Ubuntu 16.04
- VMware ESXi 6.7.0 mit VMware vSphere Web Client 6.7.0

Firewall-/NAT-Anforderungen

Wenn der virtuelle VMware SD-WAN-Edge hinter der Firewall und/oder einem NAT bereitgestellt wird, gelten die folgenden Anforderungen:

- Die Firewall muss ausgehenden Datenverkehr vom virtuellen VMware SD-WAN-Edge zu TCP/443 zulassen (für die Kommunikation mit der SD-WAN Orchestrator-Instanz).
- Die Firewall muss auf den Ports UDP/2426 (VCMP) ausgehenden Datenverkehr zum Internet zulassen.

Besondere Überlegungen für die VMware SD-WAN Virtual Edge-Bereitstellung

Beschreibt die besonderen Überlegungen für die VMware SD-WAN Virtual Edge-Bereitstellung.

- Bei SD-WAN Edge handelt es sich um eine latenzempfindliche Anwendung. Informationen dazu, wie Sie die virtuelle Maschine (VM) als latenzempfindliche Anwendung anpassen, finden Sie in der VMware-Dokumentation.
- Empfohlene Hosteinstellungen:
  - BIOS-Einstellungen, um die höchste Leistung zu erzielen:
    - CPUs mit 2,0 GHz oder höher
    - Intel Virtualization Technology (Intel VT) aktivieren
    - Hyper-Threading deaktivieren
    - Virtual Edge unterstützt paravirtualisierte vNIC VMXNET 3 und Passthrough vNIC SR-IOV:
      - Bei Verwendung von VMXNET3 deaktivieren Sie SR-IOV in Host-BIOS und ESXi
      - Bei Verwendung von SR-IOV aktivieren Sie SR-IOV in Host-BIOS und ESXi
      - Weitere Informationen zum Aktivieren von SR-IOV in VMware und KVM finden Sie unter:
        - KVM – Aktivieren von SR-IOV auf KVM
        - VMware – Aktivieren von SR-IOV auf VMware
    - Für maximale Leistung Energieeinsparungen im CPU-BIOS deaktivieren
    - CPU-Turbo aktivieren
    - Befehlssätze AES-NI, SSE3, SSE4 und RDTSC aktivieren
    - Es wird empfohlen, 2 Kerne für Hypervisor-Arbeitslasten zu reservieren

      Für ein 10-Kern-CPU-System empfiehlt es sich beispielsweise die Ausführung eines virtuellen Edge mit 8 Kernen oder von zwei virtuelle Edges mit 4 Kernen und einer Reserve von 2 Kernen für Hypervisor-Prozesse.
  - Stellen Sie bei einem Dual-Socket-Hostsystem sicher, dass der Hypervisor Netzwerkadapter, Speicher und CPU-Ressourcen zuweist, die sich innerhalb derselben Socket (NUMA)-Begrenzung wie die zugewiesenen vCPUs befinden.
- Empfohlene VM-Einstellungen:
  - 2, 4 oder 8 CPUs (dediziert)
  - 4 GB RAM für eine 2-Kern-VM, 8 GB RAM für eine 4- oder 8-Kern-VM
  - Der Arbeitsspeicher muss auf „100% reserviert“ festgelegt sein.

- Der Standardbenutzername für die SD-WAN Edge-SSH-Konsole ist `root`.

Cloud-init-Erstellung

Cloud-init ist ein Linux-Paket, das für die frühe Initialisierung von Instanzen zuständig ist. Sofern cloud-init in den Distributionen verfügbar ist, können zahlreiche gängige Parameter der Instanz direkt nach der Installation konfiguriert werden. Auf diese Weise wird eine voll funktionsfähige Instanz erstellt, die basierend auf einer Reihe von Eingaben konfiguriert wird. Die Cloud-init-Konfiguration setzt sich aus zwei Hauptkonfigurationsdateien zusammen, der Metadatendatei und der Benutzerdatendatei. Die Metadaten enthalten die Netzwerkkonfiguration für den Edge, und die Benutzerdaten enthalten die Konfiguration der Edge-Software. Die Cloud-init-Datei liefert Informationen, die die Instanz des virtuellen VMware SD-WAN-Edge identifizieren, die installiert wird.

Das Verhalten von cloud-init kann über Benutzerdaten konfiguriert werden. Benutzerdaten können vom Benutzer zum Zeitpunkt des Starts der Instanz angegeben werden. Dies geschieht in der Regel durch Anhängen einer sekundären Festplatte im ISO-Format, nach der cloud-init beim ersten Start sucht. Diese Festplatte enthält alle frühen Konfigurationsdaten, die zu diesem Zeitpunkt angewendet werden.

Der virtuelle VMware SD-WAN-Edge unterstützt cloud-init und alle wesentlichen Konfigurationen, die im Lieferumfang eines ISO-Image enthalten sind.

Erstellen der Cloud-init-Metadaten- und Benutzerdatendateien

Die Optionen für die endgültige Installationskonfiguration werden mit einem Paar von cloud-init-Konfigurationsdateien festgelegt. Die erste Installationskonfigurationsdatei enthält die Metadaten. Erstellen Sie diese Datei mit einem Texteditor und nennen Sie sie `meta-data`. Diese Datei enthält Informationen zur Identifizierung der Instanz des virtuellen VMware SD-WAN-Edge, die installiert wird. Die Instanz-ID kann ein beliebiger Name zur Identifizierung sein, und der lokale Hostname sollte ein Hostname sein, der den Standards Ihrer Site entspricht.

1 Erstellen Sie die Metadatendatei, die die Instanz `name.instance-id` enthält: `vedge1local-hostname: vedge1`

2 Erstellen Sie die Datei `network-config`, die die WAN-Konfiguration enthält. Hier müssen nur WAN-Schnittstellen angegeben werden, die eine statische IP-Adresse erfordern. Standardmäßig sind alle SD-WAN Edge-WAN-Schnittstellen für DHCP konfiguriert. Es können mehrere Schnittstellen angegeben werden.

```
root@ubuntu# cat meta-data
instance-id: Virtual-Edge
local-hostname: Virtual-Edge
network-interfaces:
      GE1:
         mac_address: 52:54:00:79:19:3d
      GE2:
         mac_address: 52:54:00:67:a2:53
```

```
      GE3:
         type: static
         ipaddr: 11.32.33.1
         mac_address: 52:54:00:e4:a4:3d
         netmask: 255.255.255.0
         gateway: 11.32.33.254
      GE4:
         type: static
         ipaddr: 11.32.34.1
         mac_address: 52:54:00:14:e5:bd
         netmask: 255.255.255.0
         gateway: 11.32.34.254
```

3 Erstellen Sie die Datei `user–data`. Diese-Datei enthält drei Hauptmodule: SD-WAN Orchestrator, den Aktivierungscode und „Zertifikatsfehler ignorieren (Ignore Certificates Errors)“.

Modul	Beschreibung
`vco`	IP-Adresse/URL der SD-WAN Orchestrator-Instanz.
`activation_code`	Aktivierungscode für den virtuellen Edge. Der Aktivierungscode wird beim Erstellen einer Edge-Instanz auf der SD-WAN Orchestrator-Instanz generiert.
`vco_ignore_cert_errors`	Option zum Überprüfen oder Ignorieren von Fehlern bei der Zertifikatsgültigkeit.

Der Aktivierungscode wird beim Erstellen einer Edge-Instanz auf der SD-WAN Orchestrator-Instanz generiert.

Wichtig Im SD-WAN Edge-Image ist kein Standardwort vorhanden. Das Kennwort muss in der Cloud-Konfiguration angegeben werden:

```
#cloud–config
password: passw0rd
chpasswd: { expire: False }
ssh_pwauth: True
velocloud:
      vce:
            vco: 10.32.0.3
            activation_code: F54F–GG4S–XGFI
            vco_ignore_cert_errors: true
```

Erstellen der ISO-Datei

Nach dem Erstellen der Dateien müssen diese in einem ISO-Image zusammengefasst werden. Dieses ISO-Image wird als virtuelle Konfigurations-CD mit der virtuellen Maschine verwendet. Dieses ISO-Image (im Beispiel unten „seed.iso“ genannt) wird mit dem folgenden Befehl auf einem Linux-System erstellt:

```
genisoimage –output seed.iso –volid cidata –joliet –rock user–data meta–data network–config
```

Das Einbeziehen der Netzwerkkonfiguration ist optional. Wenn die Datei nicht vorhanden ist, wird standardmäßig die DHCP-Option verwendet.

Sobald das ISO-Image erzeugt ist, übertragen Sie das Image in einen Datenspeicher auf dem Hostcomputer.

Installieren des virtuellen VMware SD-WAN-Edge

Sie können den virtuellen VMware SD-WAN-Edge auf KVM und VMware ESXi mithilfe einer Cloud-init-Konfigurationsdatei installieren. Die Cloud-init-Konfiguration enthält die Schnittstellenkonfigurationen und den Aktivierungsschlüssel des Edge.

Voraussetzungen

Stellen Sie sicher, dass Sie die Cloud-init-Metadatendateien und -Benutzerdatendateien erstellt und in einer ISO-Imagedatei gepackt haben. Die Schritte dazu finden Sie unter Cloud-init-Erstellung.

KVM bietet mehrere Möglichkeiten, Netzwerke für virtuelle Maschinen zur Verfügung zu stellen. VMware SD-WAN empfiehlt die folgenden Optionen:

- SR-IOV
- Linux Bridge
- OpenVSwitch Bridge

Wenn Sie den SR-IOV-Modus verwenden, aktivieren Sie SR-IOV in KVM und VMware. Die Schritte dazu finden Sie unter:

- Aktivieren von SR-IOV auf KVM
- Aktivieren von SR-IOV auf VMware

So installieren Sie den virtuellen VMware SD-WAN-Edge:

- Informationen zur Installation in KVM finden Sie unter Installieren des virtuellen Edge auf KVM.
- In VMware ESXi finden Sie weitere Informationen unter Installieren des virtuellen Edge auf VMware ESXi.

Aktivieren von SR-IOV auf KVM

Führen Sie die folgenden Schritte aus, um den SR-IOV-Modus auf KVM zu aktivieren.

Voraussetzungen

Eine bestimmte Netzwerkkarte ist erforderlich. Die folgenden Chipsätze werden von VMware SD-WAN für die Verwendung mit dem SD-WAN Gateway und SD-WAN Edge zertifiziert.

- Intel 82599/82599ES

- Intel X710/XL710

Hinweis Stellen Sie vor der Verwendung der Intel X710/XL710-Karten im SR-IOV-Modus auf KVM sicher, dass die unterstützten Firmware- und Treiber-Versionen, die im Abschnitt *Bereitstellungsvoraussetzungen* angegeben werden, ordnungsgemäß installiert sind.

So aktivieren Sie SR-IOV auf KVM:

1 Aktivieren Sie SR-IOV im BIOS. Dies hängt von Ihrem BIOS ab. Melden Sie sich bei der BIOS-Konsole an und suchen Sie nach SR-IOV-Unterstützung/DMA. Sie können die Unterstützung an der Eingabeaufforderung überprüfen, indem Sie sicherstellen, dass Intel das korrekte CPU-Flag verwendet.

```
cat /proc/cpuinfo | grep vmx
```

2 Fügen Sie die Optionen in Bboot (in `/etc/default/grub`) hinzu.

```
GRUB_CMDLINE_LINUX="intel_iommu=on"
```

   a Führen Sie folgende Befehle aus: `update–grub` und `update–initramfs –u`.

   b Neustarten

   c Stellen Sie sicher, dass IOMMU aktiviert ist.

```
velocloud@KVMperf3:~$ dmesg | grep –i IOMMU
 [ 0.000000] Command line: BOOT_IMAGE=/vmlinuz–3.13.0–107–generic root=/dev/mapper/qa––
multiboot––002––vg–root ro intel_iommu=on splash quiet vt.handoff=7
 [ 0.000000] Kernel command line: BOOT_IMAGE=/vmlinuz–3.13.0–107–generic root=/dev/mapper/qa––
multiboot––002––vg–root ro intel_iommu=on splash quiet vt.handoff=7
 [ 0.000000] Intel–IOMMU: enabled
 ….
 velocloud@KVMperf3:~$
```

3 Fügen Sie einen Treiber basierend auf dem verwendeten NIC-Chipsatz folgendermaßen hinzu:

   - Für Karten vom Typ **Intel 82599/82599ES** im SR-IOV-Modus:

     1 Laden Sie den **ixgbe**-Treiber von der Intel-Website herunter und installieren Sie ihn.

     2 Konfigurieren Sie die ixgbe-Datei (tar- und sudo-Installation).

```
velocloud@KVMperf1:~$ cat /etc/modprobe.d/ixgbe.conf
```

     3 Wenn die ixgbe-Konfigurationsdatei nicht vorhanden ist, müssen Sie die Datei folgendermaßen erstellen.

```
options ixgbe max_vfs=32,32
options ixgbe allow_unsupported_sfp=1
options ixgbe MDD=0,0
blacklist ixgbevf
```

     4 Führen Sie den Befehl `update–initramfs –u` aus und starten Sie den Server neu.

5 Verwenden Sie den Befehl `modinfo`, um sicherzustellen, dass die Installation erfolgreich verlaufen ist.

```
velocloud@KVMperf1:~$ modinfo ixgbe and ip link
 filename: /lib/modules/4.4.0-62-generic/updates/drivers/net/ethernet/intel/ixgbe/ixgbe.ko
 version: 5.0.4
 license: GPL
 description: Intel(R) 10GbE PCI Express Linux Network Driver
 author: Intel Corporation, <linux.nics@intel.com>
 srcversion: BA7E024DFE57A92C4F1DC93
```

- Für Karten vom Typ **Intel X710/XL710** im SR-IOV-Modus:
  1 Laden Sie den **i40e**-Treiber von der Intel-Website herunter und installieren Sie ihn.
  2 Erstellen Sie die virtuellen Funktionen (VFs).

```
echo 4 > /sys/class/net/device name/device/sriov_numvfs
```

  3 Um die VFs nach dem Neustart dauerhaft zu übernehmen, fügen Sie den Befehl aus dem vorherigen Schritt zur Datei "`/etc/rc.d/rc.local`" hinzu.
  4 Setzen Sie den VF-Treiber auf die Verweigerungsliste.

```
echo “blacklist i40evf” >> /etc/modprobe.d/blacklist.conf
```

  5 Führen Sie den Befehl `update-initramfs -u` aus und starten Sie den Server neu.

Validieren von SR-IOV (optional)

Sie können schnell feststellen, ob SR-IOV auf der Hostmaschine aktiviert ist, indem Sie folgenden Befehl ausführen:

```
lspci | grep –i Ethernet
```

Überprüfen Sie, ob virtuelle Funktionen verfügbar sind:

```
01:10.0 Ethernet controller: Intel Corporation 82599 Ethernet Controller Virtual Function(rev 01)
```

Installieren des virtuellen Edge auf KVM

Beschreibt die Installation und Aktivierung des virtuellen Edge auf KVM mithilfe einer cloud-init-Konfigurationsdatei.

Wenn Sie den SR-IOV-Modus verwenden, aktivieren Sie SR-IOV in KVM. Die Schritte dazu finden Sie unter Aktivieren von SR-IOV auf KVM.

So führen Sie den virtuellen VMware SD-WAN-Edge auf KVM mithilfe von „libvirt“ aus:

1 Verwenden Sie gunzip, um die Datei `qcow2` in den Image-Speicherort (z. B. `/var/lib/libvirt/images`) zu extrahieren.

2 Erstellen Sie die für das Gerät zu verwendenden Netzwerkpools mithilfe von SR-IOV und OpenvSwitch.

Verwenden von SR-IOV (Using SR-IOV)

Nachfolgend finden Sie ein Beispiel für eine Netzwerkschnittstellen-Vorlage, die speziell für Netzwerkkarten vom Typ Intel X710/XL710 mit SR-IOV verwendet wird.

```
    <interface type='hostdev' managed='yes'>
        <mac address='52:54:00:79:19:3d'/>
        <driver name='vfio'/>
        <source>
            <address type='pci' domain='0x0000' bus='0x83' slot='0x0a' function='0x0'/>
        </source>
        <model type='virtio'/>
    </interface>
```

Verwenden von OpenvSwitch (Using OpenVSwitch)

```
<network>
 <name>passthrough</name>
 <model type='virtio'/>
 <forward mode="bridge"/>
 <bridge name="passthrough"/>
 <virtualport type='openvswitch'>
 </virtualport>
 <vlan trunk='yes'>
 <tag id='33' nativeMode='untagged'/>
 <tag id='200'/>
 <tag id='201'/>
 <tag id='202'/>
 </vlan>
 </network>
 Bridge
 <network>
 <name>passthrough</name>
 <model type='virtio'/>
 <forward mode="bridge"/>
 </network>
<domain type='kvm'>
 <name>vedge1</name>
 <memory unit='KiB'>4194304</memory>
 <currentMemory unit='KiB'>4194304</currentMemory>
 <vcpu placement='static'>2</vcpu>
 <resource>
 <partition>/machine</partition>
 </resource>
 <os>
 <type arch='x86_64' machine='pc-i440fx-trusty'>hvm</type>
 <boot dev='hd'/>
 </os>
 <features>
 <acpi/>
 <apic/>
```

```
 <pae/>
 </features>
<!--
Set the CPU mode to host model to leverage all the available features on the host CPU
-->
 <cpu mode='host-model'>
 <model fallback='allow'/>
 </cpu>
 <clock offset='utc'/>
 <on_poweroff>destroy</on_poweroff>
 <on_reboot>restart</on_reboot>
 <on_crash>restart</on_crash>
 <devices>
 <emulator>/usr/bin/kvm-spice</emulator>
 <!--
 Below is the location of the qcow2 disk image
 -->
 <disk type='file' device='disk'>
 <driver name='qemu' type='qcow2'/>
 <source file='/var/lib/libvirt/images/edge-VC_KVM_GUEST-x86_64-2.3.0-18- R23-20161114-GA-
updatable-ext4.qcow2'/>
 <target dev='sda' bus='sata'/>
 <address type='drive' controller='0' bus='0' target='0' unit='0'/>
 </disk>
 <!--
 If using cloud-init to boot up virtual edge, attach the 2nd disk as CD-ROM
 -->
 <disk type='file' device='cdrom'>
 <driver name='qemu' type='raw'/>
 <source file='/home/vcadmin/cloud-init/vedge1/seed.iso'/>
 <target dev='sdb' bus='sata'/>
 <readonly/>
 <address type='drive' controller='1' bus='0' target='0' unit='0'/>
 </disk>
 <controller type='usb' index='0'>
 <address type='pci' domain='0x0000' bus='0x00' slot='0x01' function='0x2'/>
 </controller>
 <controller type='pci' index='0' model='pci-root'/>
 <controller type='sata' index='0'>
 <address type='pci' domain='0x0000' bus='0x00' slot='0x05' function='0x0'/>
 </controller>
 <controller type='ide' index='0'>
 <address type='pci' domain='0x0000' bus='0x00' slot='0x01' function='0x1'/>
 </controller>
 <!--
 The first two interfaces are for the default L2 interfaces, NOTE VLAN support just for SR-IOV
and OpenvSwitch
 -->
 < interfacetype='network'>
 < modeltype='virtio'/>
 < sourcenetwork='LAN1'/>
 < vlan>< tagid='#hole2_vlan#'/></ vlan>
 < aliasname=LAN1/>
 < addresstype='pci' domain='0x0000' bus='0x00' slot='0x12' function='0x0'/>
 </ interface>
```

```
 < interfacetype='network'>
 < modeltype='virtio'/>
 < sourcenetwork=LAN2/>
 < vlan>< tagid='#LAN2_VLAN#'/></ vlan>
 < aliasname='hostdev1'/>
 < addresstype='pci' domain='0x0000' bus=' 0x00' slot='0x13' function='0x0'/>
 </ interface>
<!--
 The next two interfaces are for the default L3 interfaces. Note that additional 6 routed
interfaces
are supported for a combination of 8 interfaces total
 -->
 < interfacetype='network'>
 < modeltype='virtio'/>
 < sourcenetwork=WAN1/>
 < vlan>< tagid='#hole2_vlan#'/></ vlan>
 < aliasname=LAN1/>
 < addresstype='pci' domain='0x0000' bus='0x00' slot='0x12' function='0x0'/>
 </ interface>
 < interfacetype='network'>
 < modeltype='virtio'/>
 < source network=LAN2/>
 < vlan>< tag id='#LAN2_VLAN#'/></ vlan>
 < aliasname='hostdev1'/>
 < addresstype='pci' domain='0x0000' bus='0x00' slot='0x13' function='0x0'/>
 </ interface>
 <serial type='pty'>
 <target port='0'/>
 </serial>
 <console type='pty'>
 <target type='serial' port='0'/>
 </console>
 <input type='mouse' bus='ps2'/>
 <input type='keyboard' bus='ps2'/>
 <graphics type='vnc' port='-1' autoport='yes' listen='127.0.0.1'>
 <listen type='address' address='127.0.0.1'/>
 </graphics>
 <sound model='ich6'>
 <address type='pci' domain='0x0000' bus='0x00' slot='0x04' function='0x0'/>
 </sound>
 <video>
 <model type='cirrus' vram='9216' heads='1'/>
 <address type='pci' domain='0x0000' bus='0x00' slot='0x02' function='0x0'/>
 </video>
 <memballoon model='virtio'>
 <address type='pci' domain='0x0000' bus='0x00' slot='0x06' function='0x0'/>
 </memballoon>
 </devices>
 </domain>
```

3 Speichert die XML-Domänendatei, die die VM definiert (z. B. die in Schritt 2 erstellte Datei `vedge1.xml`).

4 Starten Sie die VM, indem Sie die folgenden Schritte ausführen:

a Erstellen Sie eine VM.

```
virsh define vedge1.xml
```

b Starten Sie die VM.

```
virsh start vedge1
```

Hinweis `vedge1` ist der Name der VM, die im Element `<name>` der XML-Domänendatei definiert ist. Ersetzen Sie `vedge1` durch den von Ihnen im Element `<name>` angegebenen Namen.

5 Wenn Sie den SR-IOV-Modus verwenden, legen Sie nach dem Starten der VM Folgendes für die verwendeten virtuellen Funktionen (VFs) fest:

a Deaktivieren Sie den Spoofcheck.

```
ip link set eth1 vf 0 spoofchk off
```

b Aktivieren Sie den vertrauenswürdigen Modus.

```
ip link set dev eth1 vf 0 trust on
```

c Richten Sie bei Bedarf das VLAN ein.

```
ip link set eth1 vf 0 vlan 3500
```

Hinweis Der Schritt für die Konfiguration der virtuellen Funktionen gilt nicht für den OpenvSwitch (OVS)-Modus.

6 Beziehen Sie die Konsole in die VM ein.

```
virsh list
Id Name State
----------------------------------------------------
25 test_vcg running
velocloud@KVMperf2$ virsh console 25
Connected to domain test_vcg
Escape character is ^]
```

Cloud-init enthält bereits den Aktivierungsschlüssel, der beim Erstellen eines neuen virtuellen Edge im SD-WAN Orchestrator erzeugt wurde. Der virtuelle Edge wird mit den Konfigurationseinstellungen aus der Cloud-init-Datei konfiguriert. Auf diese Weise werden die Schnittstellen konfiguriert, sobald der virtuelle Edge eingeschaltet wird. Sobald der virtuelle Edge online ist, wird er mithilfe des Aktivierungsschlüssels mit dem SD-WAN Orchestrator aktiviert. Die IP-Adresse und der Aktivierungsschlüssel des SD-WAN Orchestrator wurden in der Cloud-init-Datei definiert.

Aktivieren von SR-IOV auf VMware

Die Aktivierung von SR-IOV auf VMware ist optional. Sie müssen den absoluten Nutzen von DPDK jedoch kennen, um die Leistung bei der Paketverarbeitung zu verbessern.

Voraussetzungen

Eine bestimmte Netzwerkkarte ist erforderlich. Die folgenden Chipsätze werden von VMware SD-WAN für die Verwendung mit dem SD-WAN Gateway zertifiziert.

- Intel 82599/82599ES
- Intel X710/XL710

Hinweis Stellen Sie vor der Verwendung der Intel X710/XL710-Karten im SR-IOV-Modus auf VMware sicher, dass die unterstützten Firmware- und Treiber-Versionen, die im Abschnitt *Bereitstellungsvoraussetzungen* beschrieben werden, ordnungsgemäß installiert sind.

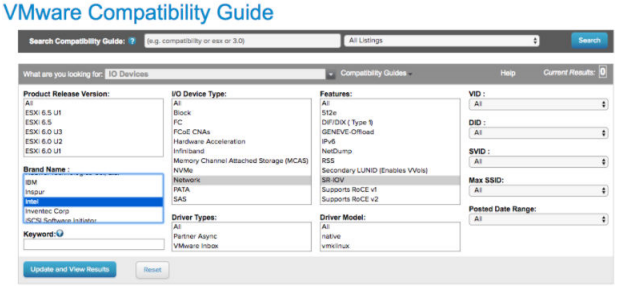
So aktivieren Sie SR-IOV auf VMware:

1 Stellen Sie sicher, dass SR-IOV von Ihrer Netzwerkkarte unterstützt wird. Überprüfen Sie die Hardwarekompatibilitätsliste (HCL) von VMware unter https://www.vmware.com/resources/compatibility/search.php?deviceCategory=io

Markenname (Brand Name): Intel

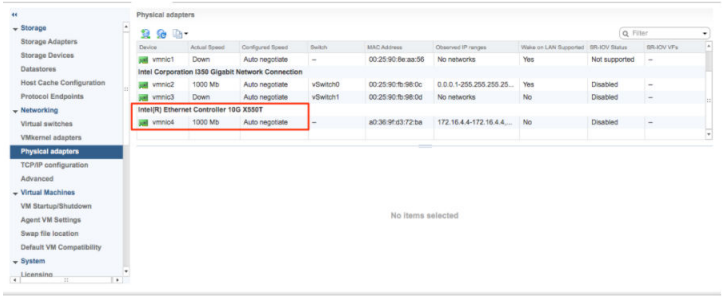
E/A-Gerätetyp (I/O Device Type): Netzwerk

Funktionen (Features): SR-IOV



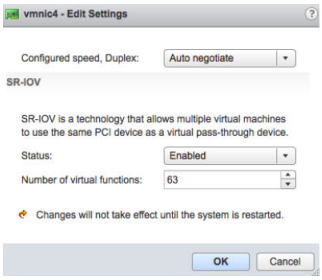
Im folgenden VMware KB-Artikel finden Sie Informationen zum Aktivieren von SR-IOV auf der unterstützten Netzwerkkarte: https://kb.vmware.com/s/article/2038739

2 Nachdem eine unterstützte Netzwerkkarte verfügbar ist, navigieren Sie zum jeweiligen VMware-Host, wählen die Registerkarte **Konfigurieren (Configure)** und dann **Physische Adapter (Physical adapters)** aus.



3 Wählen Sie **Einstellungen bearbeiten (Edit Settings)** aus. Ändern Sie **Status** in **Aktiviert (Enabled)** und geben Sie die Anzahl der notwendigen virtuellen Funktionen an. Diese Zahl variiert je nach Netzwerkkartentyp.

4 Starten Sie den Hypervisor neu.



5 Wenn SR-IOV erfolgreich aktiviert wurde, wird die Anzahl der virtuellen Funktionen (VFs) nach dem ESXi-Neustart unter der entsprechenden Netzwerkkarte angezeigt.

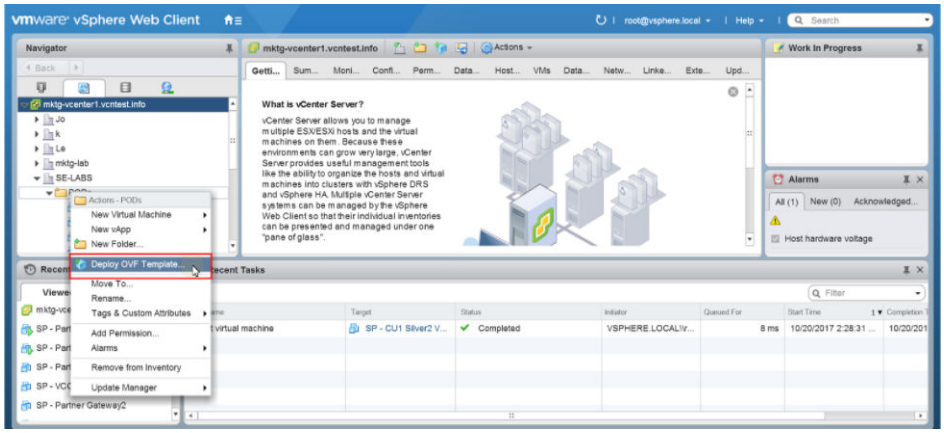
Installieren des virtuellen Edge auf VMware ESXi

Beschreibt die Installation des virtuellen Edge auf VMware ESXi.

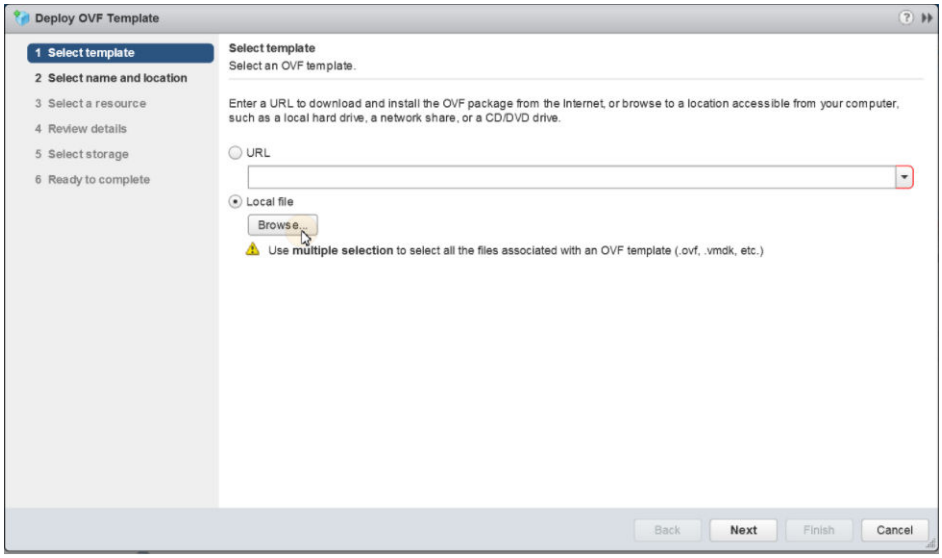
Aktivieren Sie SR-IOV auf VMware, wenn Sie den SR-IOV-Modus verwenden möchten. Die Schritte dazu finden Sie unter Aktivieren von SR-IOV auf VMware.

So installieren Sie den virtuellen Edge auf VMware ESXi:

1 Verwenden Sie den vSphere Client zum Bereitstellen einer OVF-Vorlage und wählen Sie dann die VCE-OVA-Datei aus.



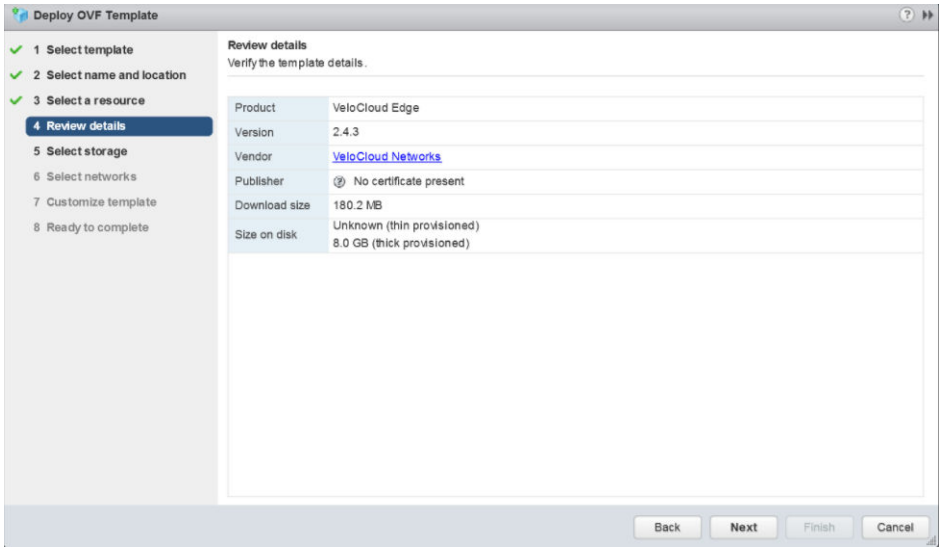
2 Wählen Sie eine OVF-Vorlage über eine URL oder eine lokale Datei aus.



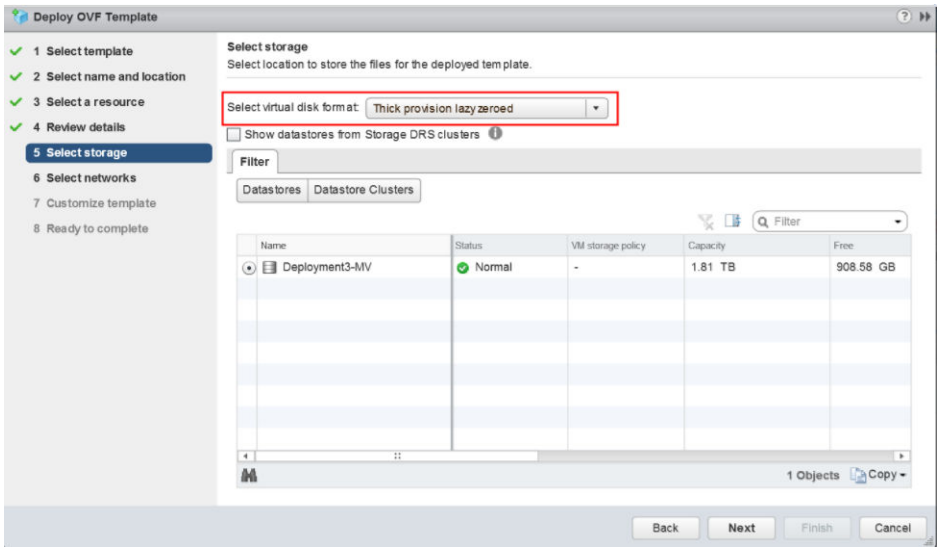
3 Wählen Sie einen Namen und einen Speicherort für die virtuelle Maschine aus.

4 Wählen Sie eine Ressource aus.

5 Überprüfen Sie die Vorlagendetails.

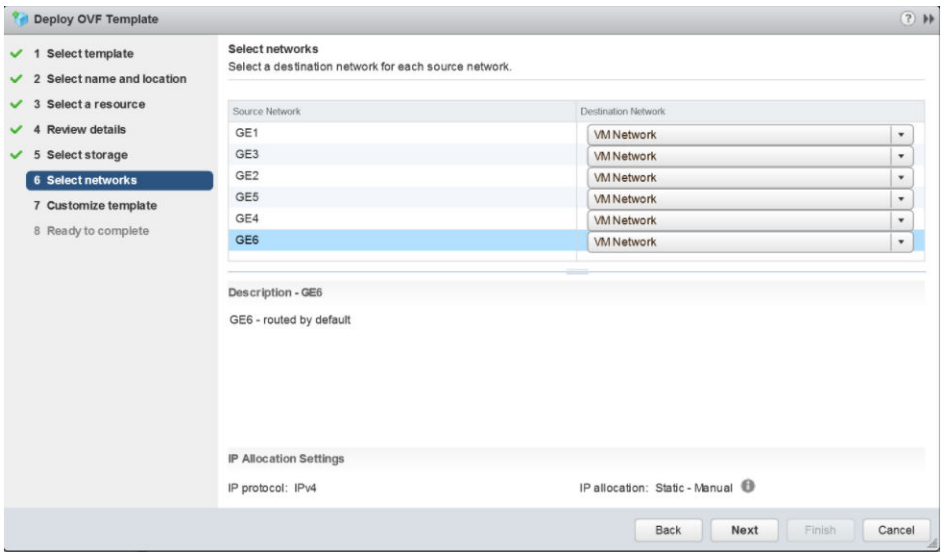


6 Wählen Sie den Speicherort zum Speichern der Dateien für die Bereitstellungsvorlage aus.



7 Konfigurieren Sie die Netzwerke für alle Schnittstellen.

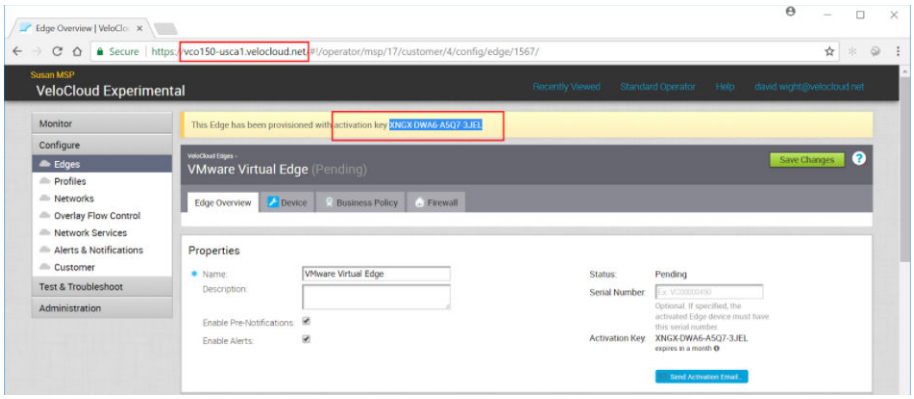
Hinweis Überspringen Sie diesen Schritt, wenn Sie eine Cloud-init-Datei zum Bereitstellen des virtuellen Edge auf ESXi verwenden.



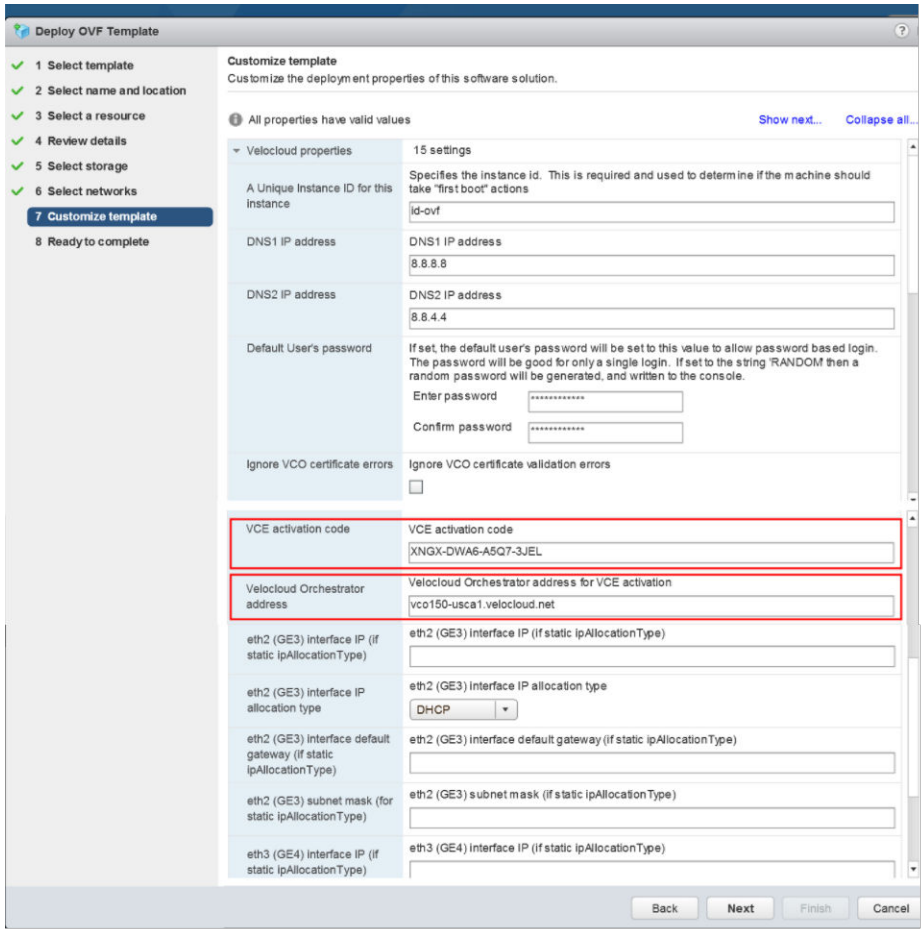
8 Passen Sie die Vorlage durch Angabe der Bereitstellungseigenschaften an. In der nachfolgenden Abbildung wird Folgendes hervorgehoben:

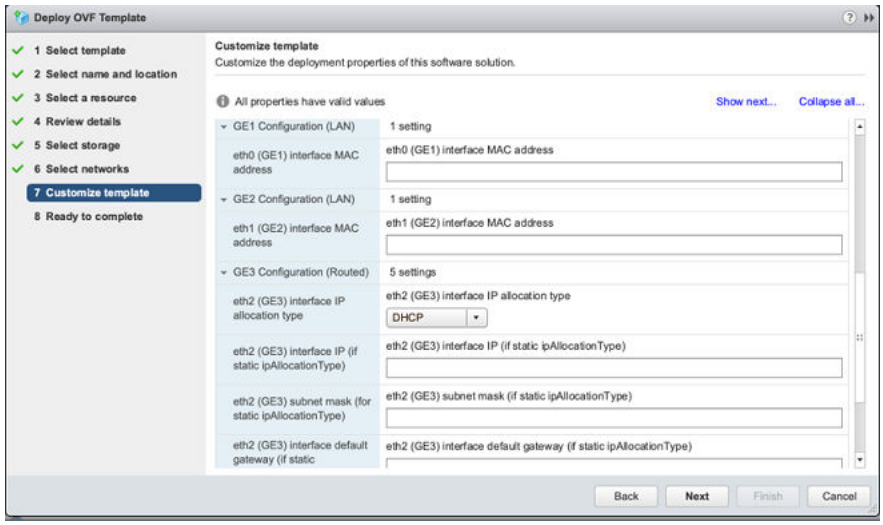
a Rufen Sie die URL/IP-Adresse aus der SD-WAN Orchestrator-Benutzeroberfläche ab. Sie benötigen diese Adresse für Schritt C (siehe unten).

b Erstellen Sie einen neuen virtuellen Edge für das Unternehmen. Nach der Erstellung des Edge kopieren Sie den Aktivierungsschlüssel. Sie benötigen den Aktivierungsschlüssel für Schritt C (siehe unten).

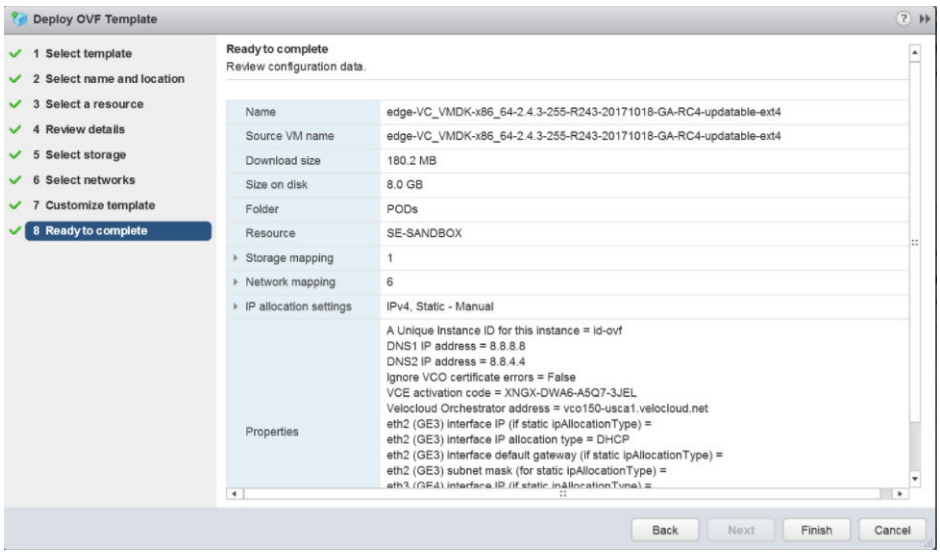


c Geben Sie auf der in folgender Abbildung angezeigten Seite „Vorlage anpassen“ den in Schritt B (siehe oben) abgerufenen Aktivierungscode und die in Schritt A (siehe oben) abgerufene URL/IP-Adresse des SD-WAN Orchestrator in den entsprechenden Feldern ein.

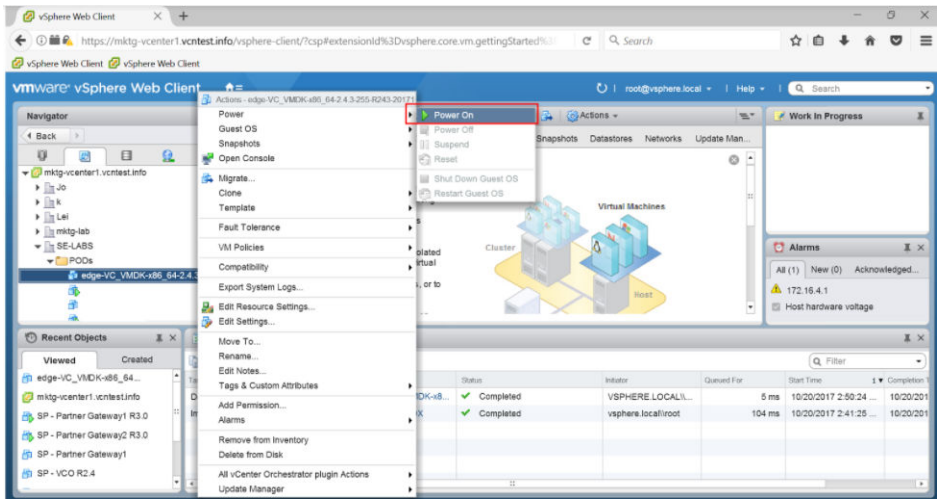




9 Überprüfen Sie die Konfigurationsdaten.



10 Schalten Sie den virtuellen Edge ein.



Nach dem Einschalten des Edge wird eine Verbindung mit dem SD-WAN Orchestrator hergestellt.

SD-WAN Gateway-Automatisierung mit Azure Virtual WAN

26

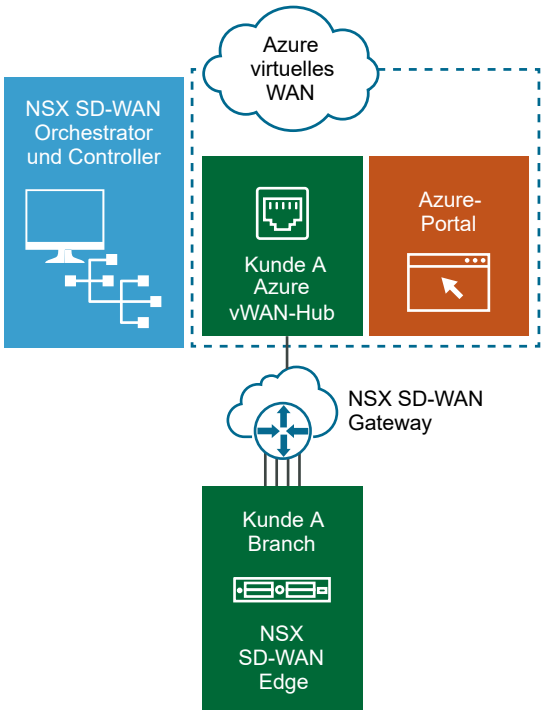
SD-WAN Orchestrator unterstützt Azure Virtual WAN und die Integration und Automatisierung von SD-WAN Gateways, um Zweigstelle-zu-Zweigstelle-VPN-Konnektivität zu ermöglichen.

Dieses Kapitel enthält die folgenden Themen:

SD-WAN Gateway-Automatisierung von Azure Virtual WAN — Übersicht

Azure Virtual WAN ist ein Netzwerkdienst, der eine optimierte und automatisierte VPN-Konnektivität (Virtual Private Network) von den Standorten der Unternehmenszweigstellen zu oder über Microsoft Azure ermöglicht. Azure-Abonnenten stellen virtuelle Hubs zur Verfügung, die den Azure-Regionen entsprechen und Zweigstellen (die SD-WAN-fähig sein können oder auch nicht) über IPSec (IP security)-VPN-Verbindungen verbinden.

SD-WAN Orchestrator unterstützt Azure Virtual WAN und die Integration und Automatisierung von SD-WAN Gateway durch Nutzung des Azure-Backbones zum Herstellen von Zweigstelle-zu-Azure-VPN-Konnektivität über das SD-WAN Gateway (siehe folgende Abbildung).



In den folgenden Abschnitten werden die Verfahren für die Konfiguration der SD-WAN Orchestrator-Instanz und Azure beschrieben, um die Zweigstelle-zu-Azure-VPN-Konnektivität über das SD-WAN Gateway zu aktivieren:

- Konfigurieren von Azure Virtual WAN für Zweigstelle-zu-Azure-VPN-Konnektivität
- Konfigurieren von SD-WAN Orchestrator für die VPN-Verbindung von Zweigstelle-zu-Azure

Voraussetzungen für die Konfiguration von Azure

Administratoren von Unternehmensnetzwerken müssen die folgenden vorausgesetzten Konfigurationsaufgaben im Azure-Portal durchführen, um sicherzustellen, dass die Anwendung SD-WAN Orchestrator zum Zweck der Integration von Azure Virtual WAN und SD-WAN Gateway als Dienstprinzipal (Identität für die Anwendung) fungieren kann.

- Registrieren der SD-WAN Orchestrator-Anwendung
- Zuweisen der SD-WAN Orchestrator-Anwendung zur Rolle „Mitwirkender (Contributor)“
- Registrieren eines Ressourcenanbieters
- Erstellen eines geheimen Clientschlüssels

Registrieren der SD-WAN Orchestrator-Anwendung

Beschreibt, wie eine neue Anwendung in Azure Active Directory (AD) registriert wird.

So registrieren Sie eine neue Anwendung in Azure AD:

Voraussetzungen

- Stellen Sie sicher, dass Sie über ein Azure-Abonnement verfügen. Falls nicht, erstellen Sie ein kostenloses Konto.

Verfahren

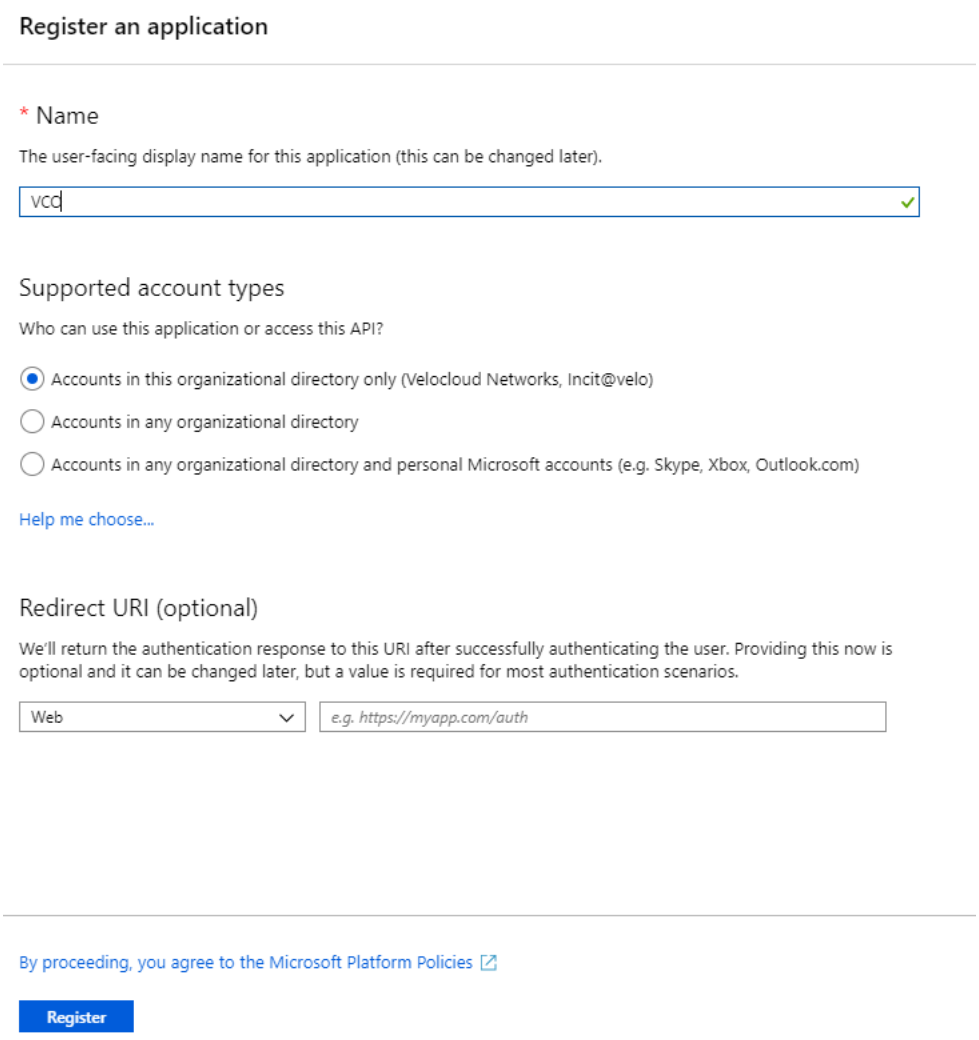
1 Melden Sie sich bei Ihrem Microsoft Azure-Konto an.

Der **Microsoft Azure**-Startbildschirm wird angezeigt.

2 Klicken Sie auf **Alle Dienste (All Services)** und suchen Sie nach **Azure Active Directory**.

3 Wählen Sie **Azure Active Directory** aus und navigieren Sie zu **App-Registrierungen (App registrations)** > **Neue Registrierung (New registration)**.

Der Bildschirm **Anwendung registrieren (Register application)** wird angezeigt.



4 Geben Sie im Feld **Name** den Namen für Ihre SD-WAN Orchestrator-Anwendung ein.

5 Wählen Sie einen unterstützten Kontotyp aus, der festlegt, wer die Anwendung verwenden kann.

6 Klicken Sie auf **Registrieren (Register)**.

Ergebnisse

Ihre SD-WAN Orchestrator-Anwendung wird registriert und auf der Registerkarte **Alle Anwendungen (All applications)** und **Eigene Anwendungen (Owned applications)** angezeigt.

Notieren Sie die Verzeichnis-ID (Mandant) und die Anwendungs-ID (Client), die bei der SD-WAN Orchestrator-Konfiguration für IaaS-Abonnements verwendet werden sollen.

Nächste Schritte

- Zuweisen der SD-WAN Orchestrator-Anwendung zur Rolle „Mitwirkender (Contributor)“
- Erstellen eines geheimen Clientschlüssels

Zuweisen der SD-WAN Orchestrator-Anwendung zur Rolle „Mitwirkender (Contributor)“

Um auf Ressourcen in Ihrem Azure-Abonnement zugreifen zu können, müssen Sie die Anwendung einer Rolle zuweisen. Sie können den Geltungsbereich auf der Ebene des Abonnements, der Ressourcengruppe oder der Ressource festlegen. Berechtigungen werden auf niedrigere Ebenen des Geltungsbereichs vererbt.

So weisen Sie die Rolle „Mitwirkender (Contributor)“ im Geltungsbereich des Abonnements zu:

Voraussetzungen

- Stellen Sie sicher, dass Sie über ein Azure-Abonnement verfügen. Falls nicht, erstellen Sie ein kostenloses Konto.

Verfahren

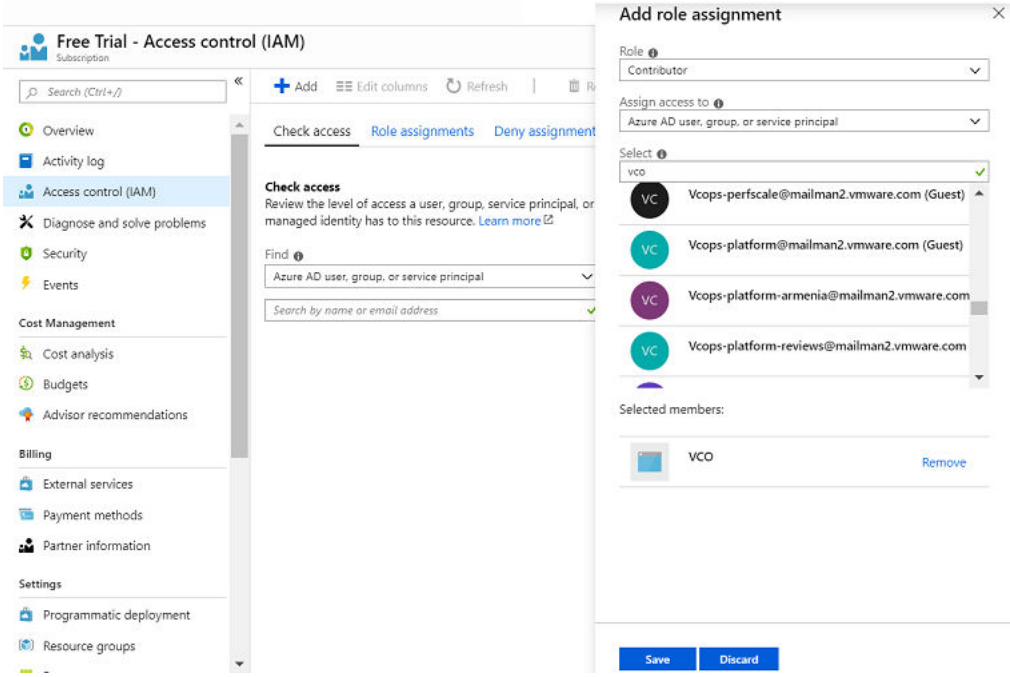
1 Klicken Sie auf **Alle Dienste (All Services)** und suchen Sie nach **Abonnements (Subscriptions)**.

2 Wählen Sie in der Abonnementliste das Abonnement aus, dem Sie Ihre Anwendung zuweisen möchten. Wenn Sie das von Ihnen gesuchte Abonnement nicht sehen, wählen Sie **Globaler Abonnementfilter (global subscriptions filter)** aus. Stellen Sie sicher, dass das gewünschte Abonnement für das Portal ausgewählt ist.

3 Klicken Sie auf **Zugriffssteuerung (Access Control) (IAM)**.

4 Klicken Sie auf **+Hinzufügen (+Add)** > **Rollenzuweisung hinzufügen (Add role assignment)**.

Das Dialogfeld **Rollenzuweisung hinzufügen (Add role assignment)** wird angezeigt.



5 Wählen Sie im Dropdown-Menü **Rolle (Role)** die Rolle **Mitwirkender (Contributor)** aus, die der Anwendung zugewiesen werden soll.

   Damit die Anwendung Aktionen wie **Neustarten (reboot)**, **Starten (start)** und **Beenden (stop)** ausführen kann, wird empfohlen, dass die Benutzer die Rolle **Mitwirkender (Contributor)** zur Anwendungsregistrierung zuweisen.

6 Wählen Sie im Dropdown-Menü **Zugriff zuweisen zu (Assign access to)** die Option **Azure AD-Benutzer, -Gruppe oder -Dienstprinzipal (Azure AD user, group, or service principal)** aus.

   Azure AD-Anwendungen werden standardmäßig nicht in den verfügbaren Optionen angezeigt. Um Ihre Anwendung zu finden, suchen Sie nach dem Dateinamen und wählen Sie ihn aus.

7 Wählen Sie **Speichern (Save)** aus.

Ergebnisse

Die Anwendung ist der Rolle „Mitwirkender (Contributor)“ zugewiesen und wird in der Liste der Benutzer angezeigt, die einer Rolle für diesen Geltungsbereich zugewiesen sind.

Nächste Schritte

- Erstellen eines geheimen Clientschlüssels
- Konfigurieren von Azure Virtual WAN für Zweigstelle-zu-Azure-VPN-Konnektivität

Registrieren eines Ressourcenanbieters

Um Virtual WAN-VPN-Konfigurationen (Virtual Private Network) herunterzuladen, benötigt der SD-WAN Orchestrator ein Blob-Speicher-Konto, das als zwischengeschalteter Datenspeicher agiert, aus dem die Konfigurationen heruntergeladen werden können. Der SD-WAN Orchestrator

hat das Ziel, eine nahtlose Benutzererfahrung zu schaffen, indem ein vorübergehendes Speicherkonto für jede der Download-Aufgaben bereitgestellt wird. Um VPN-Standortkonfigurationen herunterzuladen, müssen Sie den Ressourcenanbieter **Microsoft.Storage** manuell in Ihrem Azure-Abonnement registrieren. Standardmäßig ist der Ressourcenanbieter **Microsoft.Storage** nicht in Azure-Abonnements registriert.

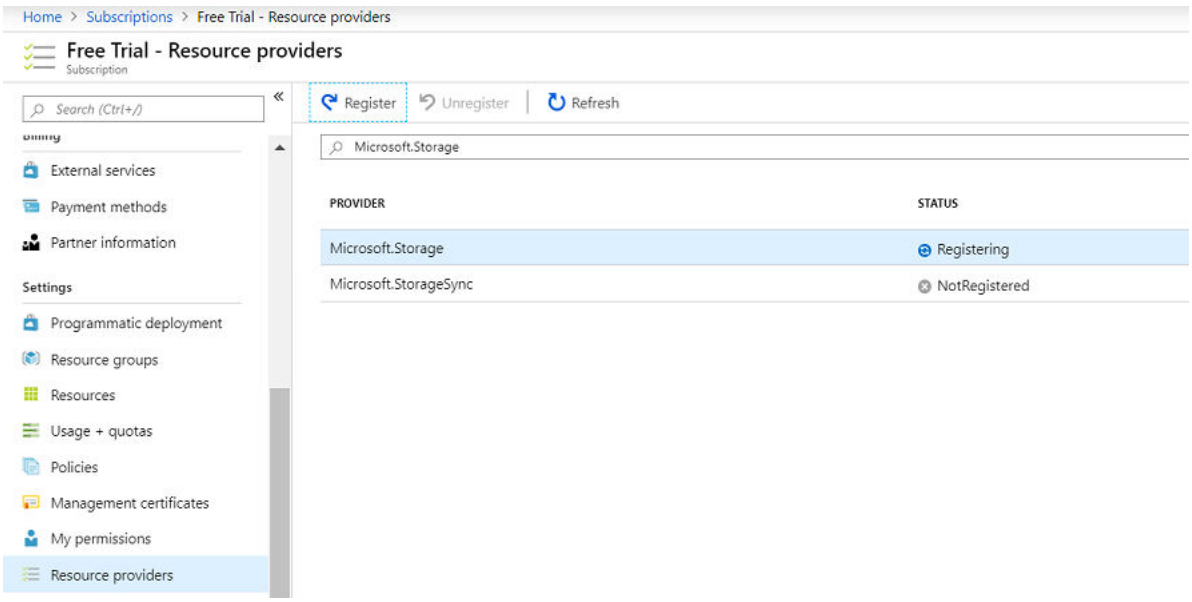
So registrieren Sie einen Ressourcenanbieter für Ihr Abonnement:

Voraussetzungen

- Stellen Sie sicher, dass Sie über ein Azure-Abonnement verfügen. Falls nicht, erstellen Sie ein kostenloses Konto.
- Stellen Sie sicher, dass Sie über die Berechtigung der Rolle „Mitwirkender“ oder „Besitzer“ verfügen.

Verfahren

1. Melden Sie sich bei Ihrem Microsoft Azure-Konto an.
2. Klicken Sie auf **Alle Dienste (All Services)** und suchen Sie nach **Abonnements (Subscriptions)**.
3. Wählen Sie in der Abonnementliste Ihr Abonnement aus.
4. Wählen Sie auf der Registerkarte **Einstellungen (Settings)** die Option **Ressourcenanbieter (Resource providers)** aus.



5. Wählen Sie in der Liste der verfügbaren Ressourcenanbieter **Microsoft.Storage** aus und klicken Sie auf **Registrieren (Register)**.

Ergebnisse

Der Ressourcenanbieter wird registriert, und Ihr Abonnement wird für die Zusammenarbeit mit dem Ressourcenanbieter konfiguriert.

Nächste Schritte

Sie können die Ressourcen in Azure erstellen. Die Schritte dazu finden Sie unter Konfigurieren von Azure Virtual WAN für Zweigstelle-zu-Azure-VPN-Konnektivität.

Erstellen eines geheimen Clientschlüssels

In diesem Abschnitt wird beschrieben, wie Sie zum Zweck der Authentifizierung einen neuen geheimen Clientschlüssel in Azure AD erstellen.

So erstellen Sie einen neuen geheimen Clientschlüssel in Azure AD:

Voraussetzungen

- Stellen Sie sicher, dass Sie über ein Azure-Abonnement verfügen. Falls nicht, erstellen Sie ein kostenloses Konto.

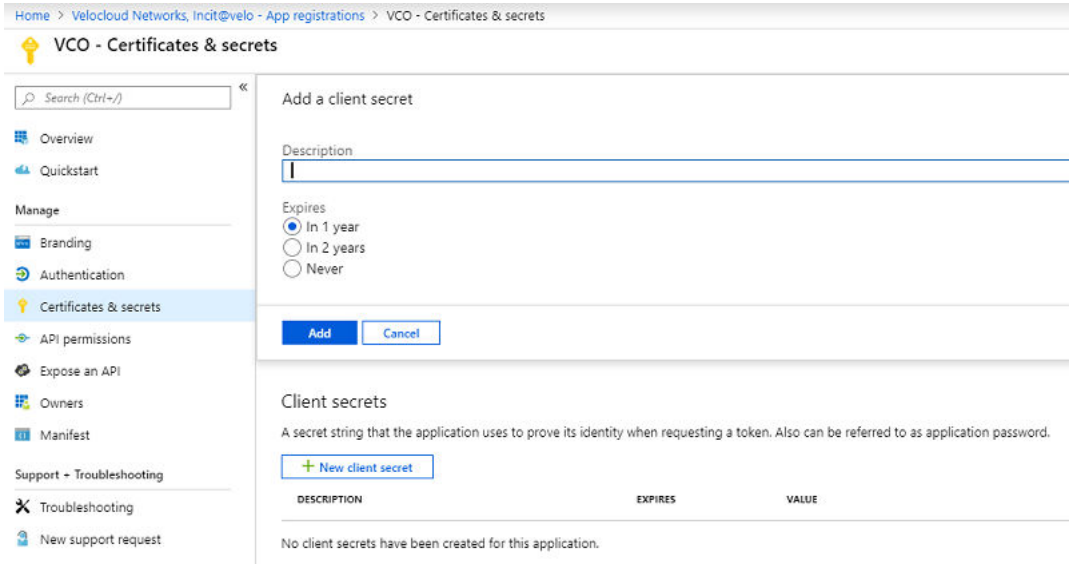
Verfahren

1. Melden Sie sich bei Ihrem Microsoft Azure-Konto an.

   Der **Microsoft Azure**-Startbildschirm wird angezeigt.

2. Wählen Sie **Azure Active Directory** > **App-Registrierungen (App registrations)** aus.
3. Klicken Sie auf der Registerkarte **Eigene Anwendungen (Owned applications)** auf Ihre registrierte SD-WAN Orchestrator-Anwendung.
4. Navigieren Sie zu **Zertifikate und geheime Schlüssel (Certificates & secrets)** > **Neuer geheimer Schlüssel (New client secret)**.

   Der Bildschirm **Neuen geheimen Clientschlüssel hinzufügen (Add a client secret)** wird angezeigt.



5 Geben Sie Details wie Beschreibung und Ablaufwert des geheimen Schlüssels an und klicken Sie auf **Hinzufügen (Add)**.

Ergebnisse

Der geheime Clientschlüssel wird für die registrierte Anwendung erstellt.

Hinweis Kopieren Sie den neuen Wert des geheimen Clientschlüssels, der im Rahmen des IaaS-Abonnements in SD-WAN Orchestrator verwendet werden soll, und speichern Sie ihn.

Nächste Schritte

- Konfigurieren von Azure Virtual WAN für Zweigstelle-zu-Azure-VPN-Konnektivität
- Konfigurieren von SD-WAN Orchestrator für die VPN-Verbindung von Zweigstelle-zu-Azure

Konfigurieren von Azure Virtual WAN für Zweigstelle-zu-Azure-VPN-Konnektivität

In diesem Abschnitt werden die Verfahren für die Konfiguration von Azure für die Integration von Azure Virtual WAN und SD-WAN Gateway zwecks Aktivierung der Zweigstelle-zu-Azure-VPN-Konnektivität beschrieben.

Bevor Sie mit der Konfiguration von Azure Virtual WAN und den anderen Azure-Ressourcen beginnen:

- Stellen Sie sicher, dass sich keines der Subnetze Ihres lokalen Netzwerks mit den vorhandenen virtuellen Netzwerken überlappt, mit denen Sie eine Verbindung herstellen möchten. Ihr virtuelles Netzwerk benötigt kein Gateway-Subnetz und kann keine virtuellen Netzwerk-Gateways haben. Informationen zu den Schritten zum Erstellen eines virtuellen Netzwerks finden Sie unter Erstellen eines virtuellen Netzwerks.

- Rufen Sie einen IP-Adressbereich für Ihre Hub-Region ab und stellen Sie sicher, dass der Adressbereich, den Sie für die Hub-Region angeben, sich nicht mit einem Ihrer bestehenden virtuellen Netzwerke überschneidet, mit denen Sie eine Verbindung herstellen.
- Stellen Sie sicher, dass Sie über ein Azure-Abonnement verfügen. Falls nicht, erstellen Sie ein kostenloses Konto.

Eine schrittweise Anleitung über die verschiedenen Verfahren, die auf der Azure-Portalseite für die Integration von Azure Virtual WAN und SD-WAN Gateway abgeschlossen werden müssen, finden Sie unter:

- Erstellen einer Ressourcengruppe
- Erstellen eines virtuellen WAN
- Erstellen eines virtuellen Hubs
- Erstellen eines virtuellen Netzwerks
- Erstellen einer virtuellen Verbindung zwischen VNet und Hub

Erstellen einer Ressourcengruppe

In diesem Abschnitt wird beschrieben, wie Sie eine Ressourcengruppe in Azure erstellen.

So erstellen Sie eine Ressourcengruppe in Azure:

Voraussetzungen

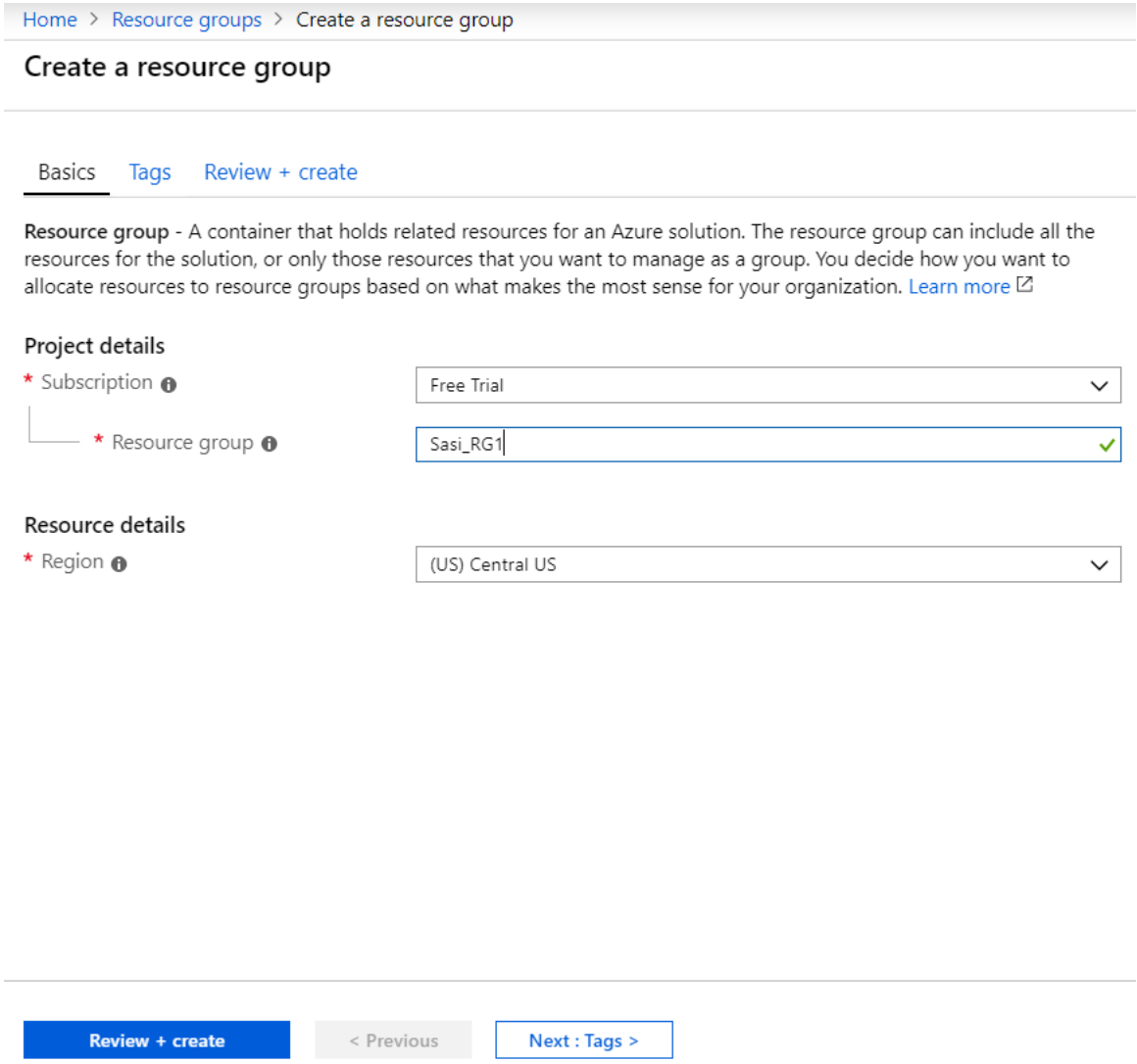
- Stellen Sie sicher, dass Sie über ein Azure-Abonnement verfügen. Falls nicht, erstellen Sie ein kostenloses Konto.

Verfahren

1. Melden Sie sich bei Ihrem Microsoft Azure-Konto an.

   Der **Microsoft Azure**-Startbildschirm wird angezeigt.
2. Klicken Sie auf **Alle Dienste (All Services)** und suchen Sie nach **Ressourcengruppen (Resource groups)**.
3. Wählen Sie **Ressourcengruppen (Resource groups)** aus und klicken Sie auf **+Hinzufügen (+Add)**.

   Der Bildschirm **Ressourcengruppe erstellen (Create a resource group)** wird angezeigt.



4 Wählen Sie im Dropdown-Menü **Abonnement (Subscription)** Ihr Microsoft Azure-Abonnement aus.

5 Geben Sie im Textfeld **Ressourcengruppe (Resource group)** einen eindeutigen Namen für Ihre neue Ressourcengruppe ein.

   Ein Ressourcengruppenname kann alphanumerische Zeichen, Punkte (.), Unterstriche (_), Bindestriche (-) und Klammern () enthalten, aber der Name darf nicht mit einem Punkt enden.

6 Wählen Sie im Dropdown-Menü **Region** den Speicherort für Ihre Ressourcengruppe aus, in dem sich die meisten Ihrer Ressourcen befinden.

7 Klicken Sie auf **Überprüfen + Erstellen (Review + Create)** und klicken Sie dann auf **Erstellen (Create)**.

Ergebnisse

Eine Ressourcengruppe wird erstellt und im Dashboard „Azure Portal (Azure portal)“ angezeigt.

Nächste Schritte

Erstellen Sie ein virtuelles WAN in Azure. Die Schritte dazu finden Sie unter Erstellen eines virtuellen WAN.

Erstellen eines virtuellen WAN

In diesem Abschnitt wird beschrieben, wie Sie ein virtuelles WAN in Azure erstellen.

So erstellen Sie ein virtuelles WAN in Azure:

Voraussetzungen

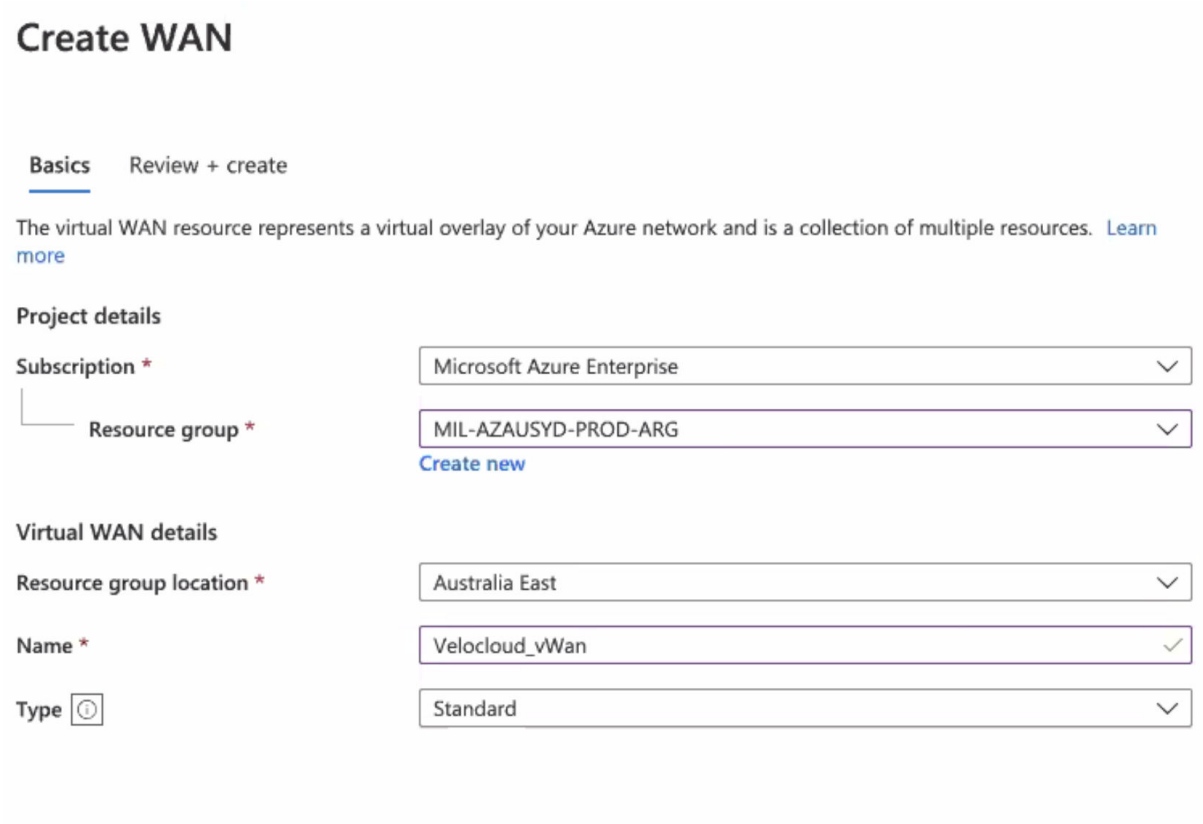
- Stellen Sie sicher, dass Sie über ein Azure-Abonnement verfügen. Falls nicht, erstellen Sie ein kostenloses Konto.
- Stellen Sie sicher, dass eine Ressourcengruppe zum Hinzufügen des virtuellen WAN erstellt wurde.

Verfahren

1. Melden Sie sich bei Ihrem Microsoft Azure-Konto an.

   Der **Microsoft Azure**-Startbildschirm wird angezeigt.
2. Klicken Sie auf **Alle Dienste (All Services)** und suchen Sie nach **Virtuelle WANs (Virtual WANs)**.
3. Wählen Sie **Virtuelle WANs (Virtual WANs)** aus und klicken Sie auf **+Hinzufügen (+Add)**.

   Der Bildschirm **WAN erstellen (Create WAN)** wird angezeigt.



4 Wählen Sie im Dropdown-Menü **Abonnement (Subscription)** Ihr Microsoft Azure-Abonnement aus.

5 Wählen Sie im Dropdown-Menü **Ressourcengruppe (Resource group)** Ihre Ressourcengruppe aus, um das virtuelle WAN hinzuzufügen.

6 Wählen Sie im Dropdown-Menü **Speicherort der Ressourcengruppe (Resource group location)** den Speicherort aus, in dem sich die Metadaten befinden, die mit dem virtuellen WAN verknüpft sind.

7 Geben Sie im Textfeld **Name** einen eindeutigen Namen für Ihr virtuelles WAN ein.

8 Wählen Sie im Dropdown-Menü **Typ (Type)** als Typ für das virtuelle WAN **Standard** aus.

9 Klicken Sie auf **Erstellen (Create)**.

Ergebnisse

Ein virtuelles WAN wird erstellt und im Dashboard „Azure Portal (Azure portal)“ angezeigt.

Nächste Schritte

Erstellen Sie virtuelle Hubs. Die Schritte dazu finden Sie unter Erstellen eines virtuellen Hubs.

Erstellen eines virtuellen Hubs

In diesem Abschnitt wird beschrieben, wie Sie einen virtuellen Hub in Azure erstellen.

So erstellen Sie einen virtuellen Hub in Azure:

Voraussetzungen

- Stellen Sie sicher, dass Sie über ein Azure-Abonnement verfügen. Falls nicht, erstellen Sie ein kostenloses Konto.
- Stellen Sie sicher, dass Sie eine Ressourcengruppe erstellt haben, um die Azure-Ressourcen hinzuzufügen.

Verfahren

1 Melden Sie sich bei Ihrem Microsoft Azure-Konto an.

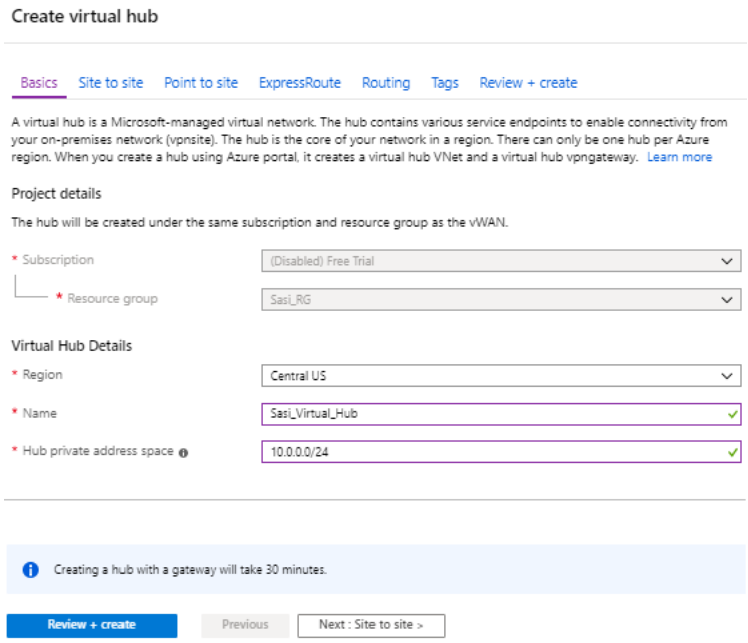
Der **Microsoft Azure**-Startbildschirm wird angezeigt.

2 Navigieren Sie zu **Alle Ressourcen (All resources)** und wählen Sie aus der Liste der verfügbaren Ressourcen das von Ihnen erstellte virtuelle WAN aus.

3 Klicken Sie im Bereich **Virtuelle WAN-Architektur (Virtual WAN Architecture)** auf **Hubs**.

4 Klicken Sie auf **+Neuer Hub (+ New Hub)**.

Der Bildschirm **Virtuellen Hub erstellen (Create virtual hub)** wird angezeigt.



5 Geben Sie auf der Registerkarte **Grundlagen (Basics)** die folgenden Details zum virtuellen Hub ein.

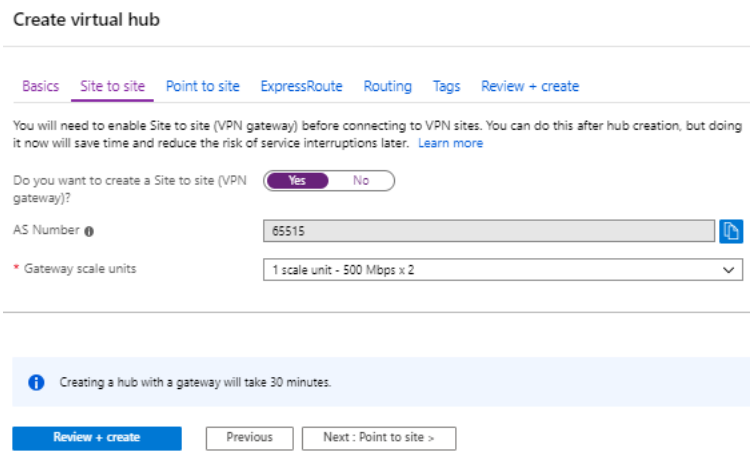
a Wählen Sie im Dropdown-Menü **Region** den Speicherort aus, an dem sich der virtuelle Hub befindet.

b Geben Sie im Textfeld **Name** den eindeutigen Namen für den Hub ein.

c Geben Sie im Textfeld **Privater Hub-Adressbereich (Hub private address space)** den Adressbereich in der CIDR (Classless inter-domain routing)-Notation ein.

6 Klicken Sie auf **Weiter: Site-to-Site > (Next: Site to site >)** und aktivieren Sie „Site-to-Site (VPN-Gateway) (Site to site (VPN gateway))“, bevor Sie eine Verbindung zu VPN-Sites herstellen, indem Sie **Ja (Yes)** auswählen.

Hinweis Ein VPN-Gateway ist erforderlich, damit die NVS-Automatisierung funktioniert. Andernfalls ist es nicht möglich, VPN-Verbindungen zu erstellen.



a Wählen Sie im Dropdown-Menü **Gateways-Skalierungseinheiten (Gateway scale units)** einen Skalierungswert aus.

7 Klicken Sie auf **Überprüfen + Erstellen (Review + Create)**.

Ergebnisse

Ein virtueller Hub wird erstellt und im Dashboard „Azure Portal (Azure portal)“ angezeigt.

Nächste Schritte

- Erstellen Sie eine virtuelle Verbindung zwischen Hubs und virtuellen Netzwerken (VNets). Die Schritte dazu finden Sie unter Erstellen einer virtuellen Verbindung zwischen VNet und Hub.
- Wenn Sie über kein vorhandenes VNet verfügen, können Sie eines erstellen, indem Sie die Schritte in Erstellen eines virtuellen Netzwerks durchführen.

Erstellen eines virtuellen Netzwerks

In diesem Abschnitt wird beschrieben, wie Sie ein virtuelles Netzwerk in Azure erstellen.

So erstellen Sie ein virtuelles Netzwerk in Azure:

Voraussetzungen

- Stellen Sie sicher, dass Sie über ein Azure-Abonnement verfügen. Falls nicht, erstellen Sie ein kostenloses Konto.

Verfahren

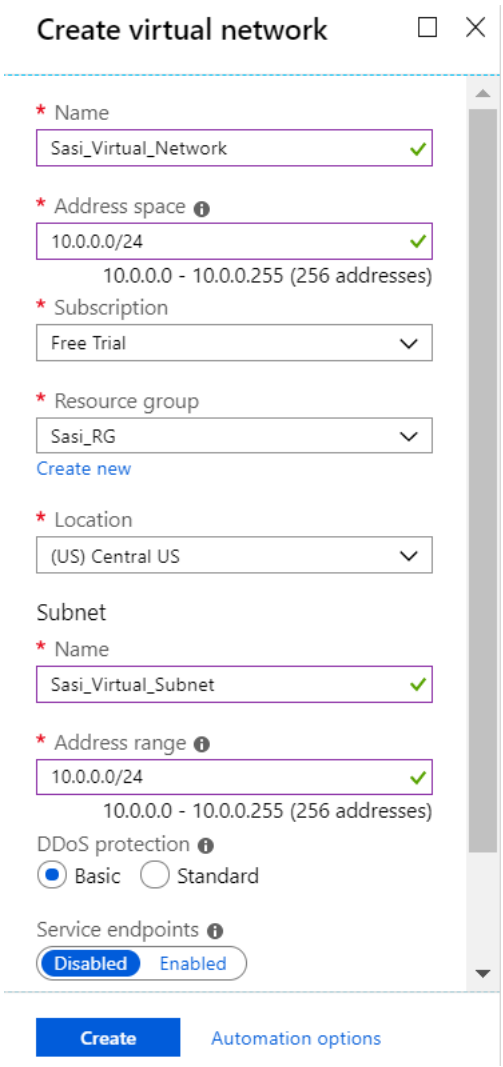
1 Melden Sie sich bei Ihrem Microsoft Azure-Konto an.

Der **Microsoft Azure**-Startbildschirm wird angezeigt.

2 Klicken Sie auf **Alle Dienste (All Services)** und suchen Sie nach **Virtuelle Netzwerke (Virtual networks)**.

3 Wählen Sie **Virtuelle Netzwerke (Virtual networks)** aus und klicken Sie auf **+Hinzufügen (+Add)**.

Der Bildschirm **Virtuelles Netzwerk erstellen (Create virtual network)** wird angezeigt.



4 Geben Sie im Textfeld **Name** den eindeutigen Namen für Ihr virtuelles Netzwerk ein.

5 Geben Sie im Textfeld **Adressbereich (Address space)** den Adressbereich für das virtuelle Netzwerk in der CIDR (Classless inter-domain routing)-Notation ein.

6 Wählen Sie im Dropdown-Menü **Abonnement (Subscription)** Ihr Microsoft Azure-Abonnement aus.

7 Wählen Sie im Dropdown-Menü **Ressourcengruppe (Resource group)** Ihre Ressourcengruppe aus, um das virtuelle Netzwerk hinzuzufügen.

8 Wählen Sie im Dropdown-Menü **Speicherort (Location)** den Speicherort aus, in dem sich das virtuelle Netzwerk befindet.

9 Geben Sie im Bereich **Subnetz (Subnet)** den Namen und Adressbereich für das Subnetz ein.

Nehmen Sie keine Änderungen an den anderen Standardeinstellungen für DDos-Schutz, Dienst-Endpoint und Firewall vor.

10 Klicken Sie auf **Erstellen (Create)**.

Ergebnisse

Ein virtuelles Netzwerk wird erstellt und im Dashboard „Azure Portal (Azure portal)“ angezeigt.

Nächste Schritte

Erstellen Sie eine virtuelle Verbindung zwischen Hubs und virtuellen Netzwerken (VNets). Die Schritte dazu finden Sie unter Erstellen einer virtuellen Verbindung zwischen VNet und Hub.

Erstellen einer virtuellen Verbindung zwischen VNet und Hub

In diesem Abschnitt wird beschrieben, wie eine virtuelle Verbindung zwischen virtuellen Netzwerken (VNets) und dem virtuellen Hub in einer bestimmten Azure-Region erstellt wird.

So erstellen Sie eine virtuelle Netzwerkverbindung zwischen einem VNet und einem virtuellen Hub in einer bestimmten Azure-Region:

Voraussetzungen

- Stellen Sie sicher, dass Sie über ein Azure-Abonnement verfügen. Falls nicht, erstellen Sie ein kostenloses Konto.
- Stellen Sie sicher, dass virtuelle Hubs und virtuelle Netzwerke erstellt wurden.

Verfahren

1 Melden Sie sich bei Ihrem Microsoft Azure-Konto an.

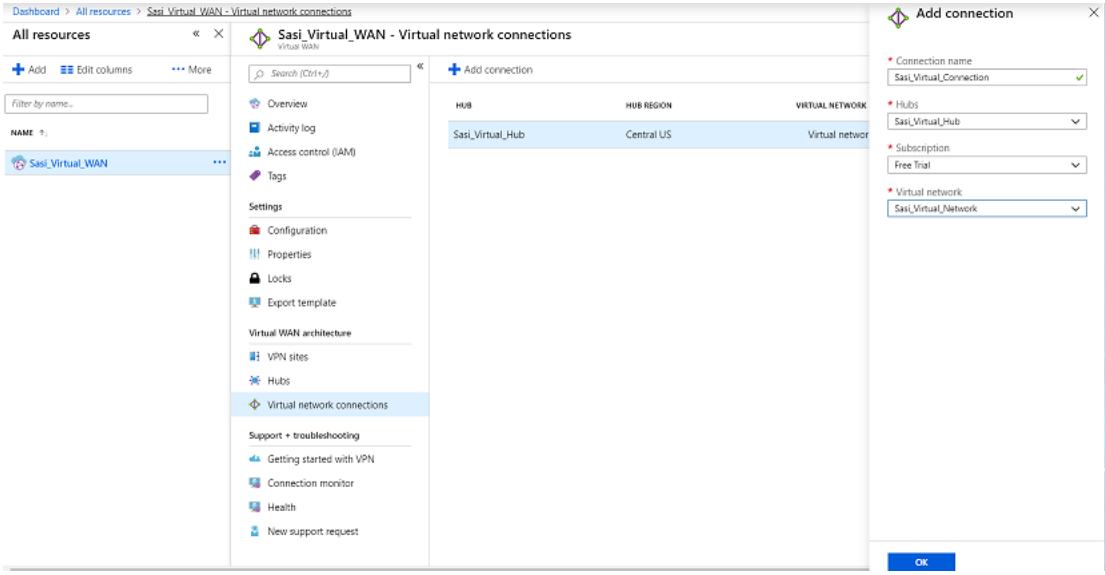
Der **Microsoft Azure**-Startbildschirm wird angezeigt.

2 Navigieren Sie zu **Alle Ressourcen (All resources)** und wählen Sie aus der Liste der verfügbaren Ressourcen das von Ihnen erstellte virtuelle WAN aus.

3 Klicken Sie unter dem Bereich **Virtuelle WAN-Architektur (Virtual WAN Architecture)** auf **Virtuelle Netzwerkverbindungen (Virtual network connections)**.

4 Klicken Sie auf **+Verbindung hinzufügen (+Add connection)**.

Der Bildschirm **Verbindung hinzufügen (Add connection)** wird angezeigt.



5 Geben Sie im Textfeld **Verbindungsname (Connection name)** den eindeutigen Namen für die virtuelle Verbindung ein.

6 Wählen Sie im Dropdown-Menü **Hubs** den Hub aus, den Sie dieser Verbindung zuordnen möchten.

7 Wählen Sie im Dropdown-Menü **Abonnement (Subscription)** Ihr Microsoft Azure-Abonnement aus.

8 Wählen Sie im Dropdown-Menü **Virtuelles Netzwerk (Virtual Network)** das virtuelle Netzwerk aus, das Sie mit diesem Hub verbinden möchten.

9 Klicken Sie auf **OK**.

Ergebnisse

Es wird eine Peering-Verbindung zwischen dem ausgewählten VNet und dem Hub hergestellt.

Nächste Schritte

- Konfigurieren von SD-WAN Orchestrator für die VPN-Verbindung von Zweigstelle-zu-Azure

Konfigurieren von SD-WAN Orchestrator für die VPN-Verbindung von Zweigstelle-zu-Azure

Sie können SD-WAN Orchestrator für die Integration von Azure Virtual WAN und SD-WAN Gateway konfigurieren, um die VPN-Verbindung von Zweigstelle-zu-Azure zu aktivieren.

Hinweis Die Funktion „Azure Virtual WAN“ ist deaktiviert. Um die Funktion zu aktivieren, müssen Sie die `session.options.enableAzureVirtualWAN`-Systemeigenschaft auf `true` festlegen.

Bevor Sie mit der SD-WAN Orchestrator-Konfiguration für Azure Virtual WAN - SD-WAN Gateway-Automatisierung beginnen, stellen Sie sicher, dass Sie alle in den Abschnitten Voraussetzungen für die Konfiguration von Azure und Konfigurieren von Azure Virtual WAN für Zweigstelle-zu-Azure-VPN-Konnektivität erläuterten Schritte abgeschlossen haben.

Eine schrittweise Anleitung über die verschiedenen Verfahren, die auf der SD-WAN Orchestrator-Seite für die Integration von Azure Virtual WAN und SD-WAN Gateway abgeschlossen werden müssen, finden Sie unter:

- Konfigurieren eines Netzwerkdiensts für ein IaaS-Abonnement
- Konfigurieren einer Microsoft Azure-Non VMware SD-WAN Site
- Synchronisieren der VPN-Konfiguration

Konfigurieren eines Netzwerkdiensts für ein IaaS-Abonnement

In diesem Abschnitt wird beschrieben, wie Sie ein Infrastructure as a Service Provider (IaaS)-Abonnement in SD-WAN Orchestrator konfigurieren.

So konfigurieren Sie ein IaaS-Abonnement in SD-WAN Orchestrator:

Voraussetzungen

Stellen Sie sicher, dass Sie die SD-WAN Orchestrator-Anwendung registriert und im Azure Portal einen geheimen Clientschlüssel erstellt haben. Informationen zu den Schritten finden Sie unter Voraussetzungen für die Konfiguration von Azure.

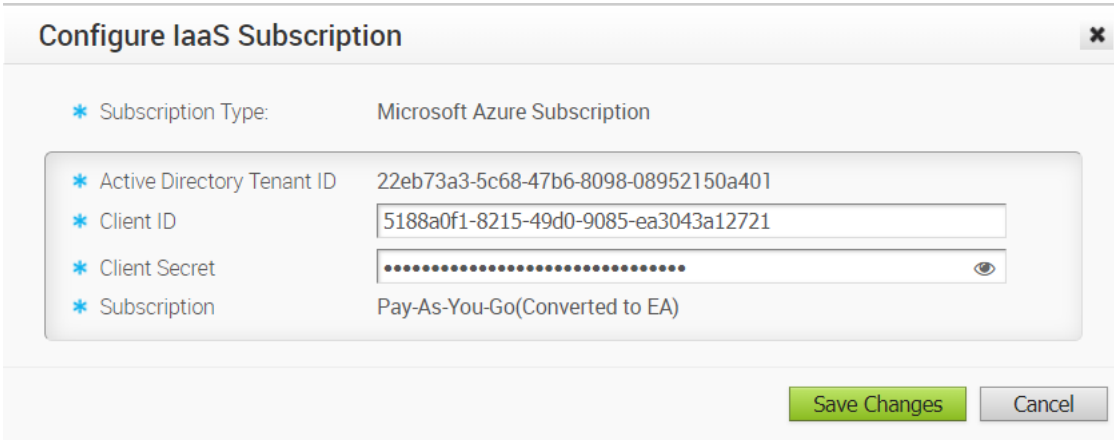
Verfahren

1 Navigieren Sie im Navigationsfenster in SD-WAN Orchestrator zu **Konfigurieren (Configure)** > **Netzwerkdienste (Network Services)**.

   Der Bildschirm **Dienste (Services)** wird angezeigt.

2 Klicken Sie im Bereich **IaaS-Abonnements (Iaas Subscriptions)** auf die Schaltfläche **Neu (New)**.

   Das Dialogfeld **IaaS-Abonnement konfigurieren (Configure IaaS Subscription)** wird angezeigt.



3 Wählen Sie im Dropdown-Menü **Abonnementtyp (Subscription Type)** die Option **Microsoft Azure-Abonnement (Microsoft Azure Subscription)** aus.

4 Geben Sie die Active Directory-Mandanten-ID, die Client-ID und den geheimen Clientschlüssel in Übereinstimmung mit Ihrer SD-WAN Orchestrator-Anwendungsregistrierung ein.

5 Klicken Sie auf die Schaltfläche **Abonnements abrufen (Get Subscriptions)**, um die Liste der Azure-Abonnements abzurufen, für die der App-Registrierung eine IAM-Rolle zugewiesen wurde.

6 Klicken Sie auf **Änderungen speichern (Save Changes)**.

Nächste Schritte

Konfigurieren Sie eine Non VMware SD-WAN Site des Typs „Microsoft Azure Virtual Hub“. Weitere Informationen finden Sie unter Konfigurieren einer Microsoft Azure-Non VMware SD-WAN Site.

Konfigurieren einer Microsoft Azure-Non VMware SD-WAN Site

In diesem Abschnitt wird beschrieben, wie eine Non VMware SD-WAN Site des Typs **Virtueller Microsoft Azure-Hub (Microsoft Azure Virtual Hub)** in SD-WAN Orchestrator konfiguriert wird.

So konfigurieren Sie einen NVS vom Typ **Virtueller Microsoft Azure-Hub (Microsoft Azure Virtual Hub)** in SD-WAN Orchestrator:

Voraussetzungen

- Stellen Sie sicher, dass Sie ein IaaS-Abonnement konfiguriert haben. Informationen zu den jeweiligen Schritten finden Sie unter Konfigurieren eines Netzwerkdiensts für ein IaaS-Abonnement.
- Stellen Sie sicher, dass Sie ein virtuelles WAN und Hubs in Azure erstellt haben. Die Schritte dazu finden Sie unter Konfigurieren von Azure Virtual WAN für Zweigstelle-zu-Azure-VPN-Konnektivität.

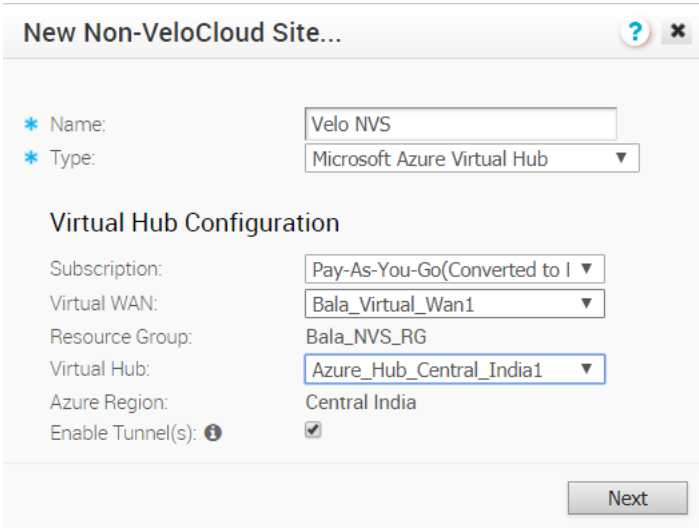
Verfahren

1 Navigieren Sie im Navigationsfenster in SD-WAN Orchestrator zu **Konfigurieren (Configure)** > **Netzwerkdienste (Network Services)**.

Der Bildschirm **Dienste (Services)** wird angezeigt.

2 Klicken Sie im Bereich „Nicht-VeloCloud-Sites (Non-VeloCloud Sites)“ auf die Schaltfläche **Neu (New)**.

Das Dialogfeld **Neue Nicht-VeloCloud-Site (New Non-VeloCloud Site)** wird angezeigt.



3 Geben Sie im Textfeld **Name** den Namen für die Non VMware SD-WAN Site ein.

4 Wählen Sie im Dropdown-Menü **Typ (Type)** den Eintrag **Virtueller Microsoft Azure-Hub (Microsoft Azure Virtual Hub)** aus.

5 Wählen Sie im Dropdown-Menü **Abonnement (Subscription)** ein Abonnement aus.

Die Anwendung ruft alle verfügbaren virtuellen WANs dynamisch von Azure ab.

6 Wählen Sie im Dropdown-Menü **Virtuelles WAN (Virtual WAN)** ein virtuelles WAN aus.

Die Anwendung füllt automatisch die Ressourcengruppe aus, der das virtuelle WAN zugeordnet ist.

7 Wählen Sie im Dropdown-Menü **Virtueller Hub (Virtual Hub)** einen virtuellen Hub aus.

Die Anwendung füllt die Azure-Region automatisch aus, die dem Hub entspricht.

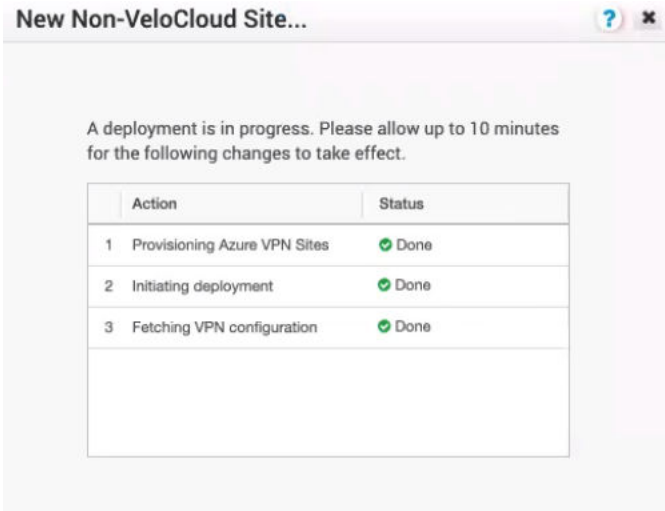
8 Aktivieren Sie das Kontrollkästchen **Tunnel aktivieren (Enable Tunnel(s))**, um VMware SD-WAN-VPN-Gateways zu ermöglichen, VPN-Tunnel zum zielseitigen virtuellen Hub zu initiieren, sobald die Site erfolgreich bereitgestellt wurde.

Hinweis VMware SD-WAN-VPN-Gateways initiieren die IKE-Verhandlung erst dann, wenn diese Non VMware SD-WAN Site auf mindestens einem Profil konfiguriert ist.

Hinweis Bei einer Non VMware SD-WAN Site vom Typ Microsoft Azure wird die öffentliche IP der SD-WAN Gateway-Schnittstelle standardmäßig als Wert für die lokale Authentifizierungs-ID verwendet.

9 Klicken Sie auf **Weiter (Next)**.

Der SD-WAN Orchestrator initiiert automatisch die Bereitstellung, stellt Azure-VPN-Tunnel bereit und lädt die Konfiguration der VPN-Site für die neu konfigurierten Sites herunter und speichert die Konfiguration in der Non VMware SD-WAN Site-Konfigurationsdatenbank von SD-WAN OrchestratorSD-WAN Orchestrator.



Ergebnisse

Sobald die Azure-VPN-Sites auf der SD-WAN Orchestrator-Seite installiert sind, können Sie die VPN-Sites (primär und redundant) im Azure-Portal anzeigen. Navigieren Sie hierfür zur Seite **Virtuelles WAN (Virtual WAN)** > **Virtuelle WAN-Architektur (Virtual WAN architecture)** > **VPN-Sites (VPN sites)**.

Nächste Schritte

- Verknüpfen Sie die Microsoft Azure Non VMware SD-WAN Site mit einem Profil, um einen Tunnel zwischen einer Zweigstelle und Azure Virtual Hub einzurichten. Weitere Informationen finden Sie unter Verknüpfen einer Non VMware SD-WAN Site mit einem Profil.
- Sie müssen SD-WAN-Routen manuell zum Azure-Netzwerk hinzufügen. Weitere Informationen finden Sie unter Bearbeiten einer VPN-Site.

Verknüpfen einer Non VMware SD-WAN Site mit einem Profil

Nach dem Konfigurieren einer Non VMware SD-WAN Site vom Typ **Virtueller Microsoft Azure-Hub (Microsoft Azure Virtual Hub)** in SD-WAN Orchestrator müssen Sie die Non VMware SD-WAN Site mit dem gewünschten Profil verknüpfen, um die Tunnel zwischen SD-WAN Gateways und dem virtuellen Microsoft Azure-Hub einzurichten.

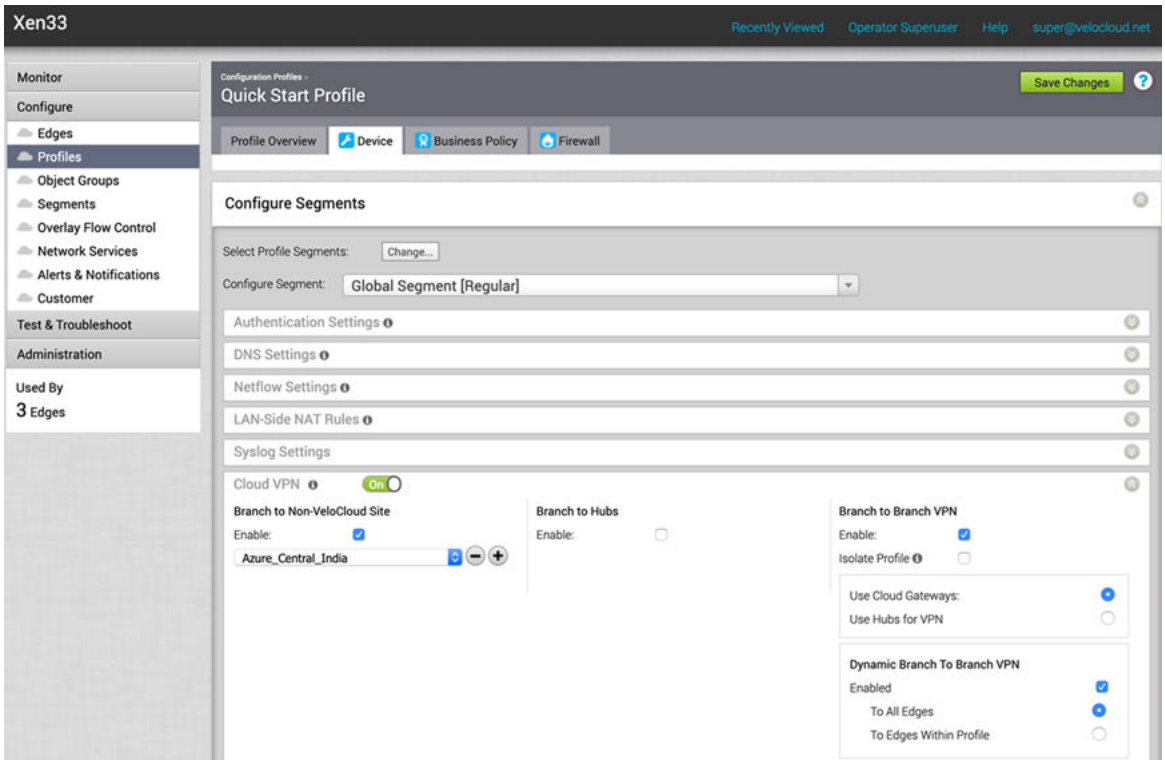
Führen Sie die folgenden Schritte aus, um eine Non VMware SD-WAN Site mit einem Profil zu verknüpfen:

Verfahren

1 Wechseln Sie im Navigationsbereich von SD-WAN Orchestrator zu **Konfigurieren (Configure)** > **Profile (Profiles)**.

Die Seite **Konfigurationsprofile (Configuration Profiles)** wird angezeigt.

2 Wählen Sie ein Profil aus, mit dem Sie die Non VMware SD-WAN Site vom Typ **Virtueller Microsoft Azure-Hub (Microsoft Azure Virtual Hub)** verknüpfen möchten, und klicken Sie auf das Symbol unter der Spalte **Gerät (Device)**.



Die Seite **Geräteeinstellungen (Device Settings)** wird für das ausgewählte Profil angezeigt.

3 Navigieren Sie zum Bereich **Cloud-VPN (Cloud VPN)** und aktivieren Sie Cloud-VPN, indem Sie die Umschaltfläche auf **Ein (On)** festlegen.

4 Aktivieren Sie unter **Zweigstelle für Nicht-VeloCloud-Site (Branch to Non-VeloCloud Site)** das Kontrollkästchen **Aktivieren (Enable)**.

5 Wählen Sie im Dropdown-Menü die Non VMware SD-WAN Site vom Typ **Virtueller Microsoft Azure-Hub (Microsoft Azure Virtual Hub)** aus, um eine VPN-Verbindung zwischen einer Zweigstelle und der Microsoft Azure Non VMware SD-WAN Site herzustellen.

6 Klicken Sie auf **Änderungen speichern (Save Changes)**.

Ergebnisse

Zwischen der Zweigstelle und der Microsoft Azure Non VMware SD-WAN Site wird ein Tunnel eingerichtet. Weitere Informationen finden Sie unter Konfigurieren einer Zweigstelle für Non VMware SD-WAN Site-VPNs.

Bearbeiten einer VPN-Site

Beschreibt, wie SD-WAN-Routen manuell zum Azure-Netzwerk hinzugefügt werden können.

So fügen Sie dem Azure-Netzwerk manuell SD-WAN-Routen hinzu:

Voraussetzungen

Stellen Sie sicher, dass Sie die Bereitstellung der Azure VPN-Sites SD-WAN Orchestrator-seitig abgeschlossen haben.

Verfahren

1 Melden Sie sich bei Ihrem Microsoft Azure-Konto an.

Der **Microsoft Azure**-Startbildschirm wird angezeigt.

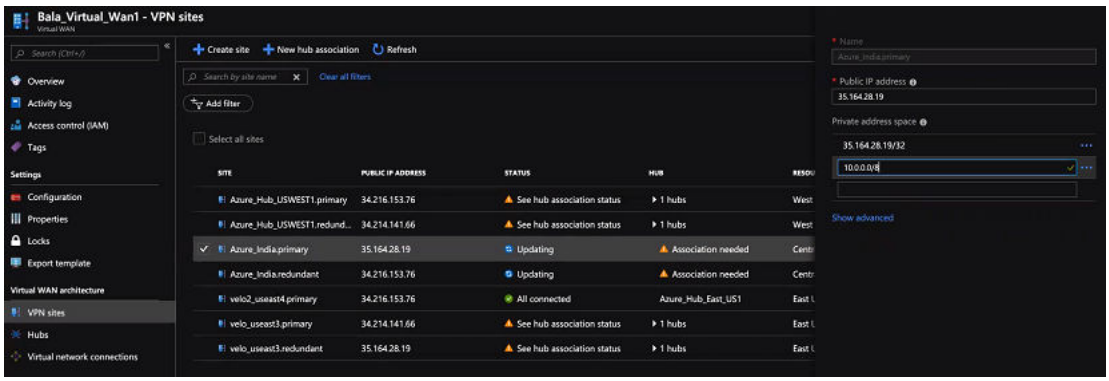
2 Navigieren Sie zu **Alle Ressourcen (All resources)** und wählen Sie aus der Liste der verfügbaren Ressourcen das von Ihnen erstellte virtuelle WAN aus.

3 Klicken Sie im Bereich **Virtuelle WAN-Architektur (Virtual WAN architecture)** auf **VPN-Sites (VPN sites)**.

4 Wählen Sie in der Liste der verfügbaren VPN-Sites die VPN-Site (z. B. *Non VMware SD-WAN Site name.primary*) aus, die während der NVS-Bereitstellung hinzugefügt wird, die mithilfe des SD-WAN Orchestrator durchgeführt wird.

5 Klicken Sie mit der rechten Maustaste auf die primäre VPN-Site und wählen Sie **Bearbeiten (Edit)** aus.

Das Popup-Fenster **Site bearbeiten (Edit site)** wird angezeigt.



6 Geben Sie im Textfeld **Privater Adressraum (Private Address Space)** den Adressbereich für die SD-WAN-Routen ein.

7 Klicken Sie auf **Bestätigen (Confirm)**.

Indem Sie die obigen Schritte durchführen, können Sie auf ähnliche Weise die redundante VPN-Site bearbeiten.

Synchronisieren der VPN-Konfiguration

Wenn nach einer erfolgreichen Non VMware SD-WAN Site-Bereitstellung Änderungen an der Endpoint-IP-Adresse des Azure Hub oder der statischen Routen vorgenommen werden, müssen Sie Azure Virtual Hub und die NVS-Konfigurationen erneut synchronisieren. Wenn Sie auf die Schaltfläche **Konfiguration erneut synchronisieren (Resync configuration)** im Bereich **Nicht-VeloCloud-Sites (Non-VeloCloud Sites)** klicken, werden die VPN-Konfigurationsdetails automatisch aus dem Azure-Portal abgerufen, und die lokale SD-WAN Orchestrator-Konfiguration wird aktualisiert.

Löschen einer Non VMware SD-WAN Site

Beschreibt die Schritte zum Löschen einer Non VMware SD-WAN Site entsprechend des virtuellen Hubs von Azure, wobei sichergestellt wird, dass der virtuelle WAN-Bereitstellungsstatus zwischen SD-WAN Orchestrator und Azure nach dem Löschvorgang konsistent ist.

Verfahren

1 Löschen Sie die Azure-VPN-Verbindungen, die mit den zu löschenden VPN-Sites verbunden sind.

2 Löschen Sie mithilfe einer Azure-API die Azure-VPN-Sites, die im Auftrag der für diesen virtuellen Hub ausgewählten Non VMware SD-WAN Site SD-WAN Gateways-Instanz bereitgestellt wurden.

Hinweis Das Löschen der Azure-VPN-Sites schlägt fehl, wenn die den VPN-Sites zugeordneten VPN-Verbindungen (die zum Löschen vorgesehen sind) nicht entfernt werden.